For Finance

Fast and Secure Connectivity from Anywhere, Designed for Financial Institutions

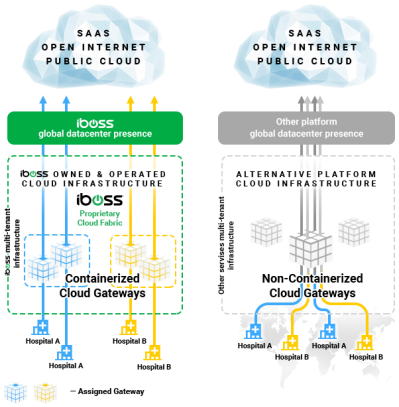
Provide Users Fast and Secure Connectivity from Anywhere with the Leading SASE Platform Based on Containerization for Complete Data Isolation

With increasing bandwidth, encrypted traffic, shifts to cloud applications like Microsoft 365 and users that are no longer constrained to traditional network boundaries, the ability to deliver fast, secure and compliant connections to cloud applications is more difficult than ever before. A Secure Access Service Edge, or SASE platform, ensures that any connection originating from a user or device to any destination in the cloud is secure and meets the organization's connectivity requirements. However, with financial regulations and security risks associated with SaaS cloud delivered platforms, leveraging a SASE platform for secure connectivity can be a challenge.

The iboss platform is the leading SASE platform that is architecturally based on containerization. Containerization allows iboss to deliver secure connectivity for users anywhere while maintaining a completely isolated and controlled network data path. In addition, a fully containerized architecture allows for natural hybrid deployments where proxy and firewall security features can be delivered within an organization's private network, while leveraging the cloud based service, if needed, for remote users or branch offices.

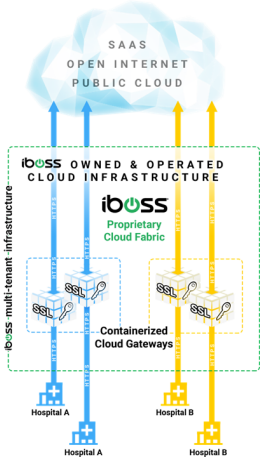
A SaaS Network Security Service with Containerization at its Core

Understanding containerization is the key for financial institutions in need of a highly secure SASE service. With a containerized service like iboss, the network connections from devices and users are processed within isolated containerized gateways which perform proxy and firewall functions. The containerized gateways never process data for any other organization and data is never mixed with that of any other customer. Containerized gateways are destroyed and created in seconds providing horizontal scaling and a global SASE fabric.



With alternative SASE platforms that lack containerization, network traffic from multiple organizations are processed within the same gateways that proxy, decrypt and firewall data for other organizations. Mixing data within the gateways that perform functions like decryption not only results in latency but increases security risks.

While Encrypted Traffic Dominates the Cloud, a Containerized Cloud Architecture Makes Inspection of that Traffic More Secure



According to the Google Transparency Report on HTTPS, 99% of all browsing time is over encrypted HTTPS connections. This requires connections to be decrypted by the SASE service to inspect content for malware, infections and data loss. To decrypt, special private key files must be used that allow traffic to be inspected and those key files must be available to the cloud gateways performing the inspection.

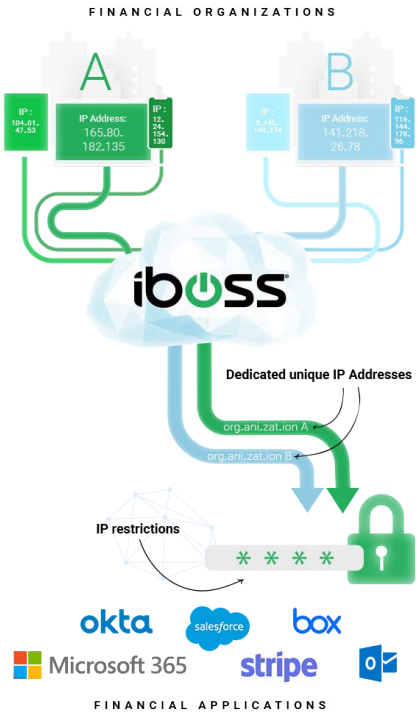
With a containerized cloud architecture like iboss, full isolation of data is achieved as it moves between users and the cloud, including full isolation of the private keys required to decrypt that traffic. The containerized cloud gateways isolate the private SSL decryption keys to ensure security and reduce risk.

With a non-containerized cloud architecture, the private SSL decryption keys must be made available to the gateways that decrypt network traffic, but those gateways are decrypting and processing traffic for any organization that traverses that gateway. This poses a big security risk as the decrypted data is now mixed within the proxies and firewalls in the cloud service. To make things worse, it provides centralized point where all SSL private keys are available so that if a key is compromised for one organization, all keys are compromised for the other organizations that the cloud gateway is servicing. This has serious implications for high-security organizations, like financial institutions.

A SASE Cloud Architecture Designed for Financial Institutions with Dedicated Source IP Addresses for Users Regardless of Location

Financial institutions need a predefined set of network security functions applied to connections from users before accessing resources. This is easier to achieve when users are onsite or within company owned and operated facilities. As users move outside of the company owned and operated network perimeter, applying needed network security functions to network connections becomes very challenging as the users are connected to untrusted networks, such as their homes or coffee shops, which are outside of the control of the financial institutions' IT staff. Network administrators do not have the advantage of configuring firewalls and routers on networks they do not control. However, the need to apply a mandatory network security stack to the connections still exists. To make things worse, the source IP Address of traffic originating from untrusted, remote networks is random and anonymous making it difficult to access restricted cloud application resources to only trusted IP sources.

The iboss platform provides a consistent network security stack that is applied to users, regardless of their location, including trusted financial organizations' operated networks and untrusted remote networks. All traffic originating from users first traverses the iboss cloud platform before making it to its final destination, including public cloud destinations and other destinations like Microsoft 365. And because the iboss platform is a SASE platform that is built on containerization, the source IP Address that is visible to the destination is always dedicated to the financial organization. This means that even if a user is working from a remote network, such as their home, when the network traffic makes it to the application, such as Microsoft 365, the source IP Address Microsoft 365 will see is that of the financial company.



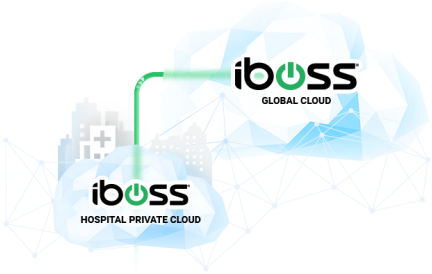
This has major advantages for financial organizations which are connecting users to trusted partners, vendors and IT platforms from locations outside of the traditional network perimeter. First, when a user connects to a cloud application service such as Microsoft 365, the company can guarantee that the network security policies their organization has in place have been applied. That is because the source IP Address is only used by users of that specific company as the containerized gateways proxy and NAT traffic without mixing data and with the ability to preserve the source IP regardless of user location.

This is unlike a non-containerized model where the source IP Addresses are shared between any customer leveraging the cloud security service. Although a security policy might be in place, it cannot be guaranteed that it is the network security policy specifically assigned by the financial institution.

Additionally, the dedicated and sticky IP Addresses provided by the iboss cloud SASE service allows the company to apply login restrictions to cloud applications making originally publicly accessible applications private. For example, a public cloud application like Microsoft 365 can be locked down to only the source IP Addresses that belong to the company provided by the iboss SASE service. Only users connected through the iboss service, and specifically connected through the agency's account, will be allowed to connect to the cloud application.

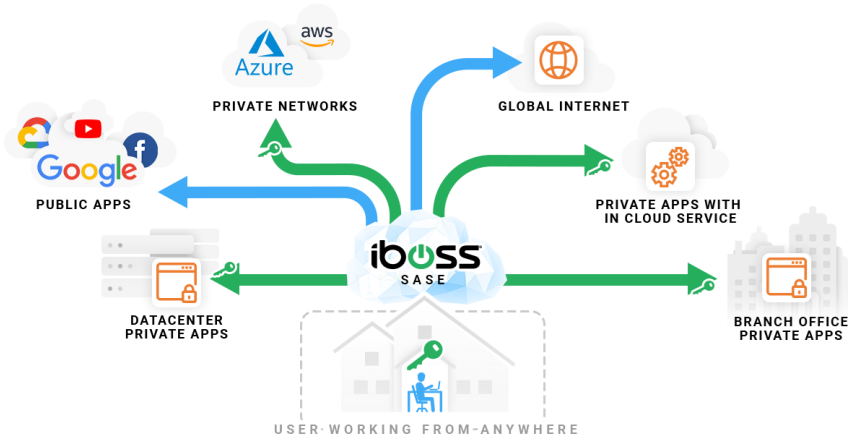
Alternatively, with a non-containerized architecture, any user leveraging the cloud SASE service, regardless of which organization they belong to, can connect to the cloud application if IP login restrictions are used. This is because the IP Addresses leveraged within the SASE service between organizations are shared and although you can lock the cloud application down to the ranges belonging to the cloud SASE service, you cannot guarantee the user accessing the front door of the application is an employee of the company. Any user running through the SASE service, belonging to any account of the SASE service, can access the application as the entire IP space of the SASE service would have to be used to lock down the cloud application front door. This also poses challenges in ensuring that the policies in place for secure and compliant network connections to cloud applications.

A Containerized SASE Architecture that is Naturally Hybrid for Easy to Deploy Private Cloud



A containerized architecture allows the containerized cloud gateways to extend into physical form so they can be run within the company's network itself. This includes running the gateways within an office or data center. The containerized gateways run on physical infrastructure that is located within the organization and have the ability to proxy and firewall traffic directly within the organization's perimeter without ever sending that traffic through the cloud gateways running within the service.

The Premier SASE Platform for Zero Trust and Cloud Security



Buy Now

The iboss cloud can secure user Internet access on any device, from any location, in the cloud. Best of all, you can start using it immediately to protect your users instantly.

What you get

- In the cloud Internet security
- Advanced Internet malware protection that follows users
- Advanced cloud and SaaS controls
- Web filtering and compliance controls
- Internet security for in-office users without appliances
- Branch office Internet security without data backhaul
- And a lot more...

Buy now

Contact Us

Get in touch with a technical specialist for a live demo.

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEIA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

Contact Us