

# Fast and Secure Connectivity from Anywhere, Designed for Government



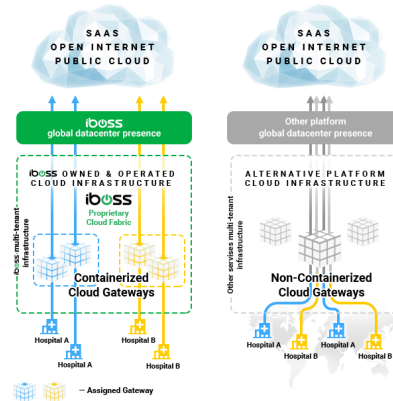
## Deliver Comply-to-Connect with the Leading SASE Platform Based on Containerization for Complete Data Isolation

With increasing bandwidth, encrypted traffic, shifts to cloud applications like Office 365 and users that are no longer constrained to the government network, the ability to deliver fast, secure and compliant connections is more difficult than ever. A Secure Access Service Edge ensures that any connection originating from a user or device to any destination in the cloud is secure and meets government connectivity requirements. However, with government 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 the government network, while leveraging the cloud based service, if needed, for remote users.

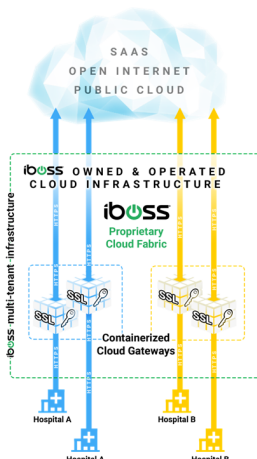
## A SaaS Network Security Service with Containerization at its Core

Understanding containerization is the key for government networks in need of a highly secure 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.



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.

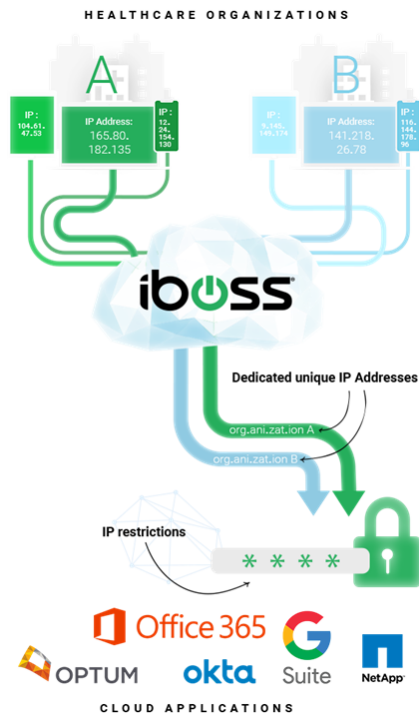
With a containerized cloud architecture like iboss, full isolation of data is achieved as it moves between users and the cloud, including full isolation of the private keys required to decrypt that traffic. The containerized cloud gateways isolate the private SSL decryption keys to ensure security and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

# A SASE Cloud Architecture Designed for Government Comply to Connect Initiatives with Dedicated Source IP Addresses for Users Regardless of Location

Government agencies working on comply to connect initiatives 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 government owned and operated facilities. As users move outside of the government 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 government agency. 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 government 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 Office 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 government agency. 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 Office 365, the source IP Address Office 365 will see is that of the government agency.

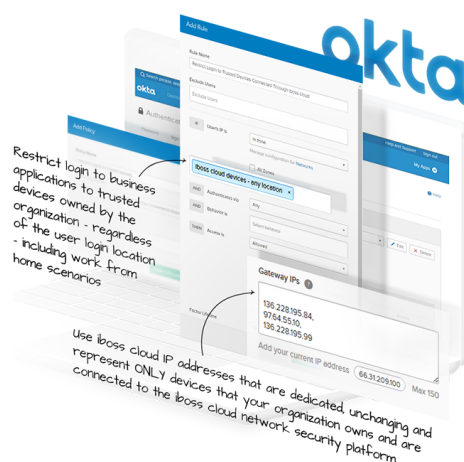


This has major advantages for government agencies which are running comply to connect initiatives. First, when a user connects to a cloud application service such as Office 365, the agency can guarantee that the network security policies that specific government agency has in place have been applied. That is because the source IP Address is only used by users of that specific government agency as the containerized gateways proxy and NAT traffic without mixing data and with the ability to preserve the source IP regardless of user location.

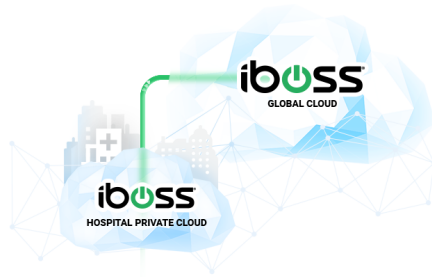
This is unlike a non-containerized model where the source IP Addresses are shared between any customer leveraging the cloud security service. Although a security policy might be in place, it cannot be guaranteed that it is the network security policy specifically assigned by the government agency.

Additionally, the dedicated and sticky IP Addresses provided by the iboss cloud SASE service allows the government agency to apply login restrictions to cloud applications making originally publicly accessible applications private. For example, a public cloud application like Microsoft Office 365 can be locked down to only the source IP Addresses that belong to the government agency. 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 agency or organization, can connect to the service if IP login restrictions are used. This is because the IP Addresses 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 that of the specific agency. 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 comply to connect initiatives are those for the specific government agency.



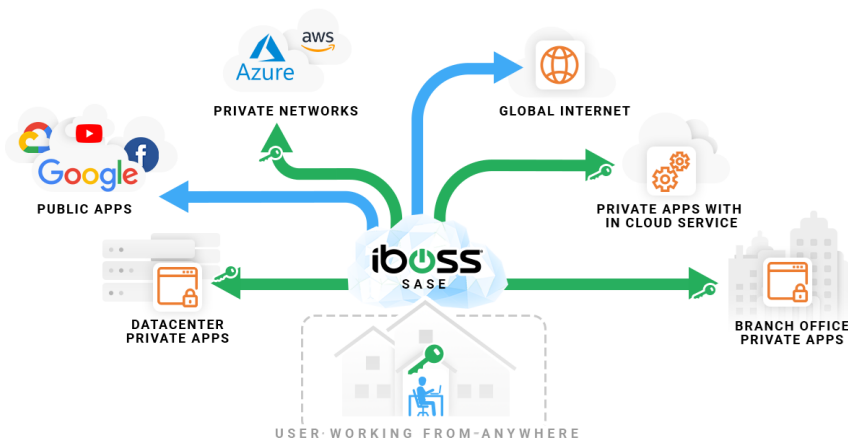
## A Containerized SASE Architecture that is Naturally Hybrid for Government Agencies



A containerized architecture allows the containerized cloud gateways to extend into physical form so they can be run within the government network itself. This includes running the gateways within a government office, base or data center. The containerized gateways run on physical infrastructure that is within the government network and have the ability to proxy and firewall traffic directly within the government facility without ever sending that traffic through the cloud gateways running within the service.

This is much different than alternative SASE services which are not based on containerization and do not have the ability to naturally extend in the private cloud form. When the iboss cloud containerized gateways run onsite, within the government network, they can be linked to the global containerized cloud footprint. This means that traffic from remote users does not have to traverse back to the government datacenter while still having the same network security policies and source IP address ranges in place that are used within the private gateways running within the government facility. Deployments can be as many private cloud gateways and iboss cloud gateways as needed and can even shift over time. This provides the flexibility to transition from an on-prem private cloud appliance model to a full SASE model over time and with ease while gaining the benefits of protecting remote workers immediately today.

## 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](mailto:sales@iboss.com)

#### International Sales:

858-568-7051 X1  
Contact local distributor or:  
[sales@iboss.com](mailto:sales@iboss.com)

#### EMEIA Sales:

+44 20 3884 0360  
Contact local distributor or:  
[emeia@iboss.com](mailto:emeia@iboss.com)

Contact Us