Private Access VPN Replacement

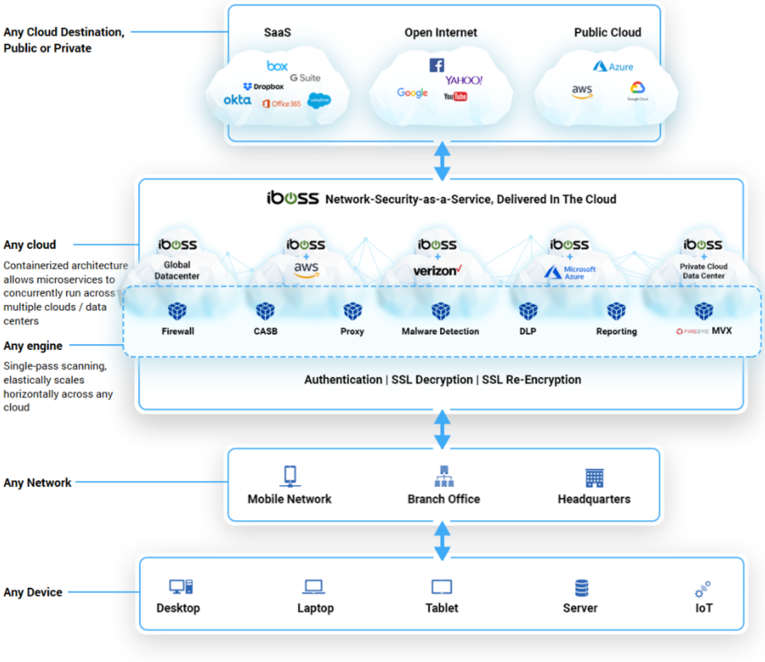
The iboss cloud Zero Trust Network Access (ZTNA) Private Access Platform architecture

Allow users to work from anywhere and connect to any cloud application, public or private, with iboss cloud

Organizations are constantly faced with competitive pressures that force them to adapt their business. While an organization's technology strategies and resources should keep pace with these changes, the reality is they often lag behind. This creates a gap between how people work and how the IT infrastructure supports them. When the gap becomes too big, many problems arise, including security risks, operational disruption, compliance violations, skyrocketing costs, and poor user experience.

Organizations deploying and using legacy network security appliances to protect cloud connectivity and internet access are faced with these problems today. Mobility, exponential bandwidth growth and cloud application adoption is leading to escalating costs, difficulty in securing users outside of the traditional network perimeter, and loss of end user productivity due to slow connections resulting from forcing traffic for remote workers through corporate networks. The physical network perimeter has eroded making devices the new network perimeter Users can work from anywhere and need fast and secure connections to all cloud resources regardless of location.

The shift to a Zero Trust network architecture allows organizations to ensure fast compliant and secure connections from any location. Because users are always connected through the cloud network security service, access to cloud applications and resources can be granted based on who the user is, including the user's role within an organization. These resources can be public or private. Public resources might include Microsoft Office 365, while private resources are those that are typically behind a firewall or within a corporate network. The iboss cloud network security service is connected to all resources and makes decisions on which resources a user might have access based on user identity.


Any Cloud Destination, Public or Private
SaaS
Open Internet
Public Cloud
box
G Suite
Dropbox
okta
Office 365
salesforce
YAHOO!
Google
YouTube
Azure
aws
iboss Network-Security-as-a-Service, Delivered In The Cloud
Any cloud
Containerized architecture allows microservices to concurrently run across multiple clouds / data centers
Any engine
Single-pass scanning, elastically scales horizontally across any cloud
iboss Global Datacenter
iboss + aws
iboss + verizon
iboss + Microsoft Azure
iboss + Private Cloud Data Center
Firewall
CASB
Proxy
Malware Detection
DLP
Reporting
FIREEYE MVX
Authentication | SSL Decryption | SSL Re-Encryption
Any Network
Mobile Network
Branch Office
Headquarters
Any Device
Desktop
Laptop
Tablet
Server
IoT

The iboss cloud platform connects users to cloud resources based on role using a Zero Trust architecture

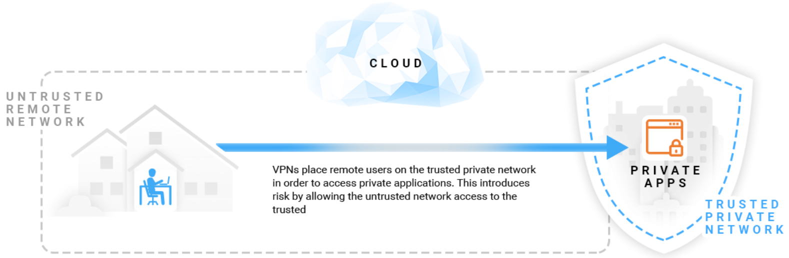
Private access falls under the Zero Trust Network Access, or ZTNA, model. Private access provides access to those resources that have no direct public access and are protected by firewalls or other restrictions. These resources are typically within a datacenter, within a corporate network or within a private virtual network inside of Azure of AWS. The iboss cloud provides role based access to these private resources to these resources based on a user' s role within an organization.

ZTNA Private Access Replaces Virtual Private Networks (VPNs)

First, it is important to understand the difference between private access provided by ZTNA and Virtual Private Networks, or VPNs. Although both provide access to private resources, the way users are granted access to those resources via iboss private access is drastically different.

We will start with a simple example to set the foundation for the concept. When watching a movie via a streaming video service like Netflix, the person watching the movie is provided access to the Netflix application which provides the movie. The end-useris not granted access to the Netflix data center network. In fact, there is zero-network access to the Netflix data center network that provides the streaming movie. The user is only granted access to the movie itself via the Netflix application.

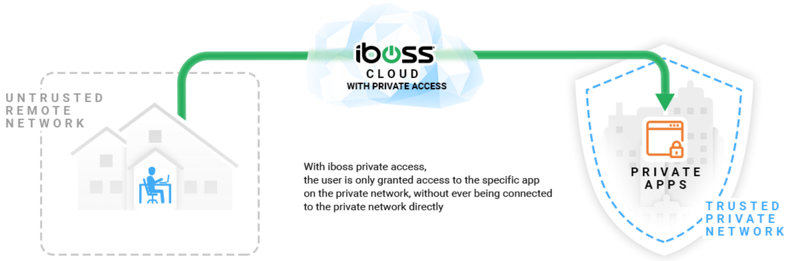
In contrast, with a traditional VPN, the user is granted access to the private corporate network to gain access to private applications. The VPN connects the user to the actual private network itself which then allows the user to connect to the private application. This is the equivalent of Netflix granting the movie watcher access to the Netflix data center network in order to access the Netflix application, which is not only unrealistic, but highly insecure.



VPNs place remote users on the trusted private network in order to access private applications. This introduces risk by allowing the untrusted network access to the trusted

With VPNs, remote users are connected from their untrusted network to the trusted network to gain access to private apps

The iboss private access service inverts the VPN model completely. Instead of granting a user access to private network, the iboss ZTNA service never places the user on any private network at all. Instead, the iboss private access service provides the user with access to the application itself, without ever granting or connecting the user directly to the network from which that application is being hosted. In fact, you can think of iboss private access as Zero Network Access, as the user never actually has access to the network itself. The iboss private access service is connected to all private resources an organization needs to grant access to and leverages this to connect users, based on their role, to the private application directly. In essence, the user can consume the application much like watching a movie on Netflix.



With iboss private access, the user is only granted access to the specific app on the private network, without ever being connected to the private network directly

iboss private access grants access to private applications without placing the remote user on the trusted private network

Users are connected through the iboss cloud service at all times, and the iboss cloud service has access to all public and private resources. It grants access to those resources based on role, and abstracts network routing and other network related complexities from the policies which grant access to those resources. It uses an Identity Provider, or IdP, to determine who the user is and which groups the user belongs to in order to provide access. For example, if the user is part of the manager's group, they may have access to private resources only available to managers.

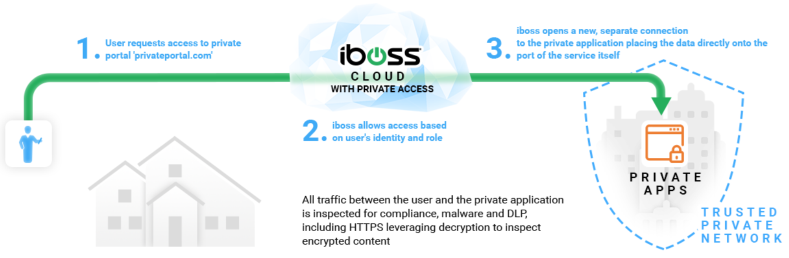
iboss Private Access Connectivity Details

In order to provide access to private resources, connections must flow through the iboss cloud platform. Connections are routed through the iboss cloud platform using an agent, called a cloud connector, which transparently intercepts network traffic and re-routes it through the iboss cloud platform before heading to the final cloud destination.

When a user requests a private cloud resource, the iboss private access service follows the following algorithm:

1. The agent routes the traffic to the iboss cloud platform for inspection
2. The iboss cloud platform determines what resource is being requested. Based on the user's identity and role, the iboss cloud platform allows or denies the request
3. If the request is allowed, the iboss service opens a new connection, separate from the original end user connection to the private resource. It places the data for the user right at the port of the private application itself
4. The platform inspects traffic as it bridges the user to the private resource application

Note in the algorithm above, there are two distinct and separate connections. The first connection is between the user and the iboss cloud platform. The second connection is between the iboss cloud platform and the private resource. This is important as it never provides a direct network connection between the user and the private resource.



1. User requests access to private portal 'privateportal.com'

2. iboss allows access based on user's identity and role

3. iboss opens a new, separate connection to the private application placing the data directly onto the port of the service itself

All traffic between the user and the private application is inspected for compliance, malware and DLP, including HTTPS leveraging decryption to inspect encrypted content

Private access provides access to any private resource based on a user's identity and role

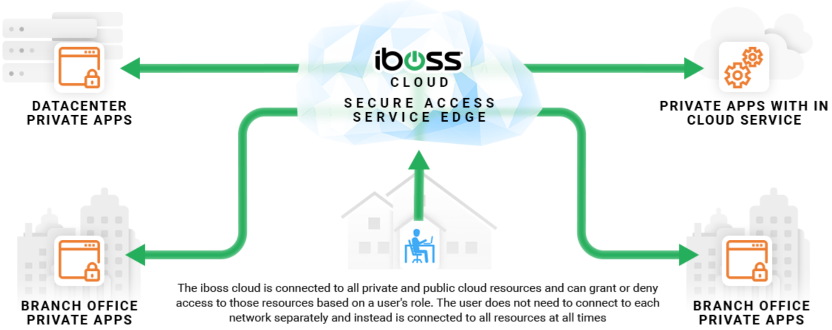
Secondly, notice the iboss cloud platform will place the data directly onto the port where the application is being offered. This is important as there is no opportunity for the end-user to scan the server across other ports as the network data is placed directly in front of the private application service, and only that application even though that service may be hosted on the same server hosting other resources.

The iboss private access service goes beyond micro network segmentation, by eliminating network access altogether. In addition, the service eliminates oeast-west• traffic on a private network as end users are never on the network eliminating east-hosting other resources.

The iboss private access service goes beyond micro network segmentation, by eliminating network access altogether. In addition, the service eliminates “east-west” traffic on a private network as end users are never on the network eliminating east-west traffic altogether.

iboss Provides a Single Point of Connectivity for All Resources, Public and Private

The iboss cloud platform provides access to both public and private resources. This simplifies user connectivity by eliminating the need for end users to privately connect to different private networks to gain access to resources across an organization. With VPNs, for example, a user may need to switch between various VPNs to gain access to various private resources hosted within different private networks, such as data centers or branch offices. With the iboss private access service, the user is transparently connected to the iboss cloud platform alone, and the iboss cloud platform is connected to everything that user might be able to access. This allows organizations to centrally grant access to various disparate private resources located in different regions, different networks, different branch offices and various public cloud providers. Users are granted access based on the user's identity and the user's role within the organization.


iboss
CLOUD
SECURE ACCESS SERVICE EDGE
DATACENTER PRIVATE APPS
PRIVATE APPS WITH IN CLOUD SERVICE
BRANCH OFFICE PRIVATE APPS
BRANCH OFFICE PRIVATE APPS

The iboss cloud is connected to all private and public cloud resources and can grant or deny access to those resources based on a user's role. The user does not need to connect to each network separately and instead is connected to all resources at all times

Instead of connecting to having to connect to different networks with a VPN, the user is connected to all private and public cloud resources at all times through iboss cloud which is connected to all resources

The Future of SD-WAN

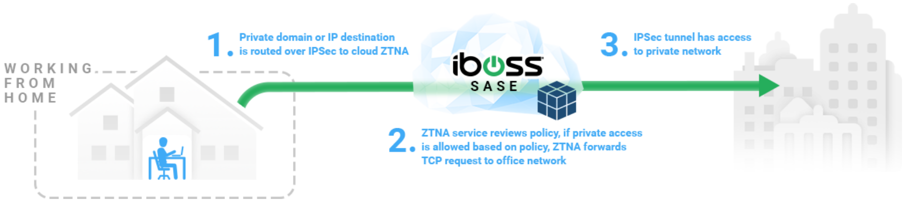
The iboss cloud platform can connect the user to private resources, regardless of whether the user is in an office or working from home. The user is always connected through the iboss cloud service which makes the location of the user less relevant. SD-WAN projects typically leverage appliances to connect offices together so that users can access resources hosted within various office locations. With iboss private access, users have access to all resources, public and private, including resources hosted within other office locations. The user is connected directly to the iboss cloud service, which bridges that user to any private resource hosted in any other office. This eliminates the need to deploy and manage SD- WAN appliances in order to connect those users to the various private resources in other offices. This forms a software-defined perimeter, or SDP, in which software connects users to various resources, not hardware. The iboss cloud private access platform is a next-gen SD-WAN replacement based on a borderless world.

Connecting private resources to iboss cloud

In order to provide access to private resources, those resources must be connected to the iboss cloud platform. The flexibility of the iboss cloud platform, which is based on containerization, allows the most options for bridging private resources to the iboss cloud service. This includes appliance-free options to bridge to private resources. The following lists the various options for connecting private resources to the iboss cloud platform:

Connectivity Method	Description
IPSec tunnels	The iboss cloud platform fully supports IPSec tunnels that can be established between branch offices and the iboss cloud service. The iboss cloud service can leverage the IPSec tunnels to connect to private resources in order to provide access to those resources to end users.
GRE tunnels	If the resources are HTTPS portals, which are already encrypted, GRE tunnels can be leveraged to bridge the iboss cloud service to the private resources. The GRE tunnel is established between the iboss cloud service and a router or firewall at the edge of the private network.
Private Cloud Containerized Gateways	The native containerized architecture allows customers to extend containerized cloud gateway capacity into private cloud. These containerized gateways perform full proxy and firewall functions and can replace traditional appliances such as Bluecoat proxies, McAfee proxies, Cisco CWS proxies and Forcepoint proxies. In addition, these private containerized gateways also have private access capabilities built-in and can form a bridge to the private network. The iboss cloud gateways will leverage the path through the private cloud containerized gateways to grant access to private resources.
Access Control Lists – ACLs	Containerization provides unique and dedicated IP addresses to be used through the iboss cloud service. Because of this, ACLs can be used to grant access to the containerized cloud gateways to private resources hosted within a private network. The ACLs contain the IP addresses of the iboss cloud gateways which are dedicated to the organization.
Azure Firewall as a Service 3P Integration	3P integration for Azure allows the iboss cloud service to natively stretch into the Azure cloud and automatically secure all network traffic entering and leaving the Azure edge without ever deploying a virtual firewall. It's a pure SaaS service that is automatically configured by the platform, including load balancing and high-availability (HA). When enabled, the containerized cloud gateways run within Azure so they can also bridge users to private resources automatically. This is one of the core advantages to the containerized as it has the ability to bridge access across any cloud, including Azure, easily.

Connecting users to private networks via IPSec tunnels and a variety of other methods is support by the iboss cloud platform.


WORKING FROM HOME
1. Private domain or IP destination is routed over IPSec to cloud ZTNA
iboss SASE
2. ZTNA service reviews policy, if private access is allowed based on policy, ZTNA forwards TCP request to office network
3. IPSec tunnel has access to private network

Users can connect to private apps and resources through iboss cloud which levergaes IPSec tunnels or private cloud gateways for access to private resources

Understanding Private Cloud Containerized Gateways

Each blade contains containerized private cloud gateways Private cloud gateways are available in other form factors, including 1U appliances

Private cloud container zed gateways run on infrastructure hosted within the data center or corporate office. When running private cloud containerized gateways, the global cloud network security fabric which runs in global POPs extends into the private POP. It provides a way to create a "Private Point of Presence." These private cloud containerized gateways have 100% of all the capabilities and features found within the cloud service, which runs containerized cloud gateways throughout the network security fabric. This results in having a fully featured proxy and firewall features baked into the private cloud gateways in addition to having private access ZTNA capabilities which can bridge users to the private cloud resources.

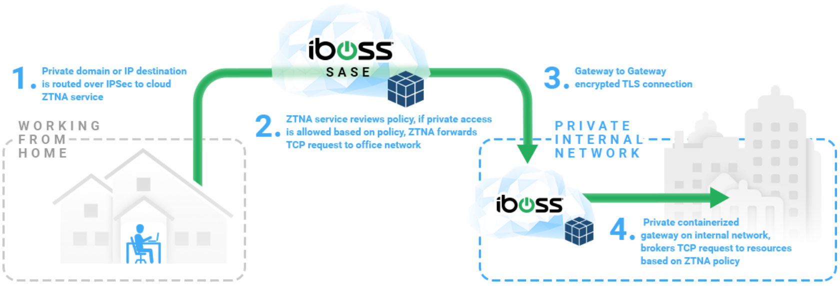
Because the private cloud containerized gateways have consolidated features beyond private access, this eliminates the need to deploy private access only appliances or virtual appliances as required by other private access vendors. This reduces costs, overhead, labor, security risks and compliance overhead by reducing niche infrastructure designed to perform a single function. The private cloud containerized gateways are also optional and used when an IPSec tunnel is not preferred. They can be deployed at the edge of the private network or within the private network itself, within a DMZ, with limited public access granted only to the global iboss cloud gateways that service the organization.

The private cloud gateways will bridge requests from users to private cloud resources. They also allow other iboss cloud gateways servicing an organization to broker requests through themselves into private resources.

The Most Advanced and Intelligent Global Network Security Fabric that Provides Users with Fast and Secure Connections to Any Application, from Anywhere

The containerized cloud gateways are always close to the end user to provide fast and secure access to any cloud resource regardless of where the user resides. Private cloud resources may only be accessible through particular gateways, however, such as those gateways where IPSec tunnels from branch offices are terminated or private cloud containerized gateways that provide a bridge to the private resource.

The global cloud fabric uses built-in intelligence to route allowed private access requests from end-users to other gateways that have access to the resource. The gateways use TLS encrypted connections to broker connections between themselves to ensure the private cloud resource is made available to the end-user regardless of location. The internal routing is 100% automatic and is handled completely by the iboss global cloud service. This includes brokering a connection from a user connected to a containerized cloud gateway through a different private cloud gateway automatically.


1. Private domain or IP destination is routed over IPSec to cloud ZTNA service
WORKING FROM HOME
iboss SASE
2. ZTNA service reviews policy, if private access is allowed based on policy, ZTNA forwards TCP request to office network
3. Gateway to Gateway encrypted TLS connection
PRIVATE INTERNAL NETWORK
iboss
4. Private containerized gateway on internal network, brokers TCP request to resources based on ZTNA policy

iboss cloud can broker requests through private cloud containerized gateways without needing IPSec tunnels

Flexible Private Access Network Topology

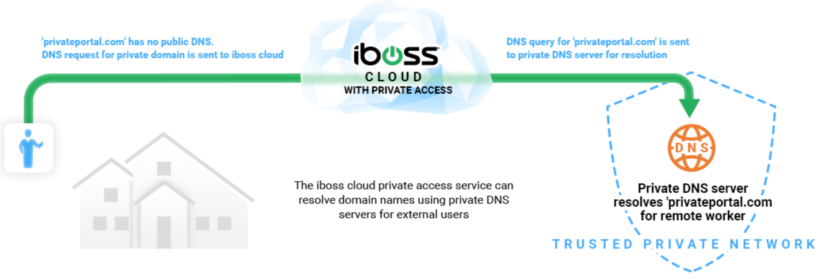
The iboss cloud private access service allows brokering to private resources via a variety of methods, including IPSec tunnels, private cloud gateways and Azure network security as a service. Because of the architecture, the private access service allows mixing the different connectivity methods to connect to different private networks using any of the available connectivity methods. For example, some private resources might be connected with IPSec tunnels while others are leveraging containerized private cloud gateways. Other private resources within Azure, including servers and vnets, might be connected automatically via Azure SaaS network security which is fully managed and configured by the cloud service without ever having to manually create a virtual machine or deploy a virtual firewall. Together, these private cloud access points provide the iboss cloud platform the ability to connect to private resources regardless of location.

Infinite Load Balancing for Private Access

Traditional VPNs can easily get saturated as the volume of VPN traffic increases from remote users. The iboss cloud private access service does not provide direct network access to end users. Instead it brokers connections for end-users by creating new connections to those resources, which originate from the cloud gateway itself. Because containerization allows for horizontal scaling, the cloud gateways can increase capacity infinitely by distributing the load across multiple IPSec tunne s which have access to the private resource or distributing load across multiple private cloud containerized gateways. Regardless of how the private resource is connected to the iboss cloud service, its horizontal scaling capability provided by the native containerized architecture means any volume of remote traffic can be hand ed with ease.

DNS Brokering for Private Resources

Many private resources do not have publicly resolvable domain names as they are not hosted on the public DNS network. The iboss cloud private service can broker DNS resolution from the end user, through the iboss cloud service, to an internal DNS server for resolution. In addition, the private cloud service has the ability to automatically broker the DNS queries to the appropriate cloud gateways that have access to the internal DNS server to make DNS resolution function appropriately, even if the end-user is not connected directly to the private network.


'privateportal.com' has no public DNS.
DNS request for private domain is sent to iboss cloud
iboss CLOUD WITH PRIVATE ACCESS
DNS query for 'privateportal.com' is sent to private DNS server for resolution
DNS
The iboss cloud private access service can resolve domain names using private DNS servers for external users
Private DNS server resolves 'privateportal.com for remote worker
TRUSTED PRIVATE NETWORK

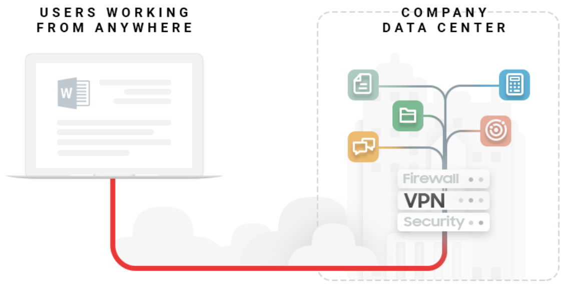
The iboss cloud private access service can resolve DNS queries for private destinations

The Most Powerful Zero Trust Connectivity Platform

The iboss cloud platform provides access to any resource, treating the user and device as the new network perimeter. With private access, this includes easily bridging users to private resources that typically would involve placing remote users on private networks which introduces major risk given those users are remote. The iboss cloud platform provides service-based access to any resource easily and transparently and is designed for the cloud-first borderless future.

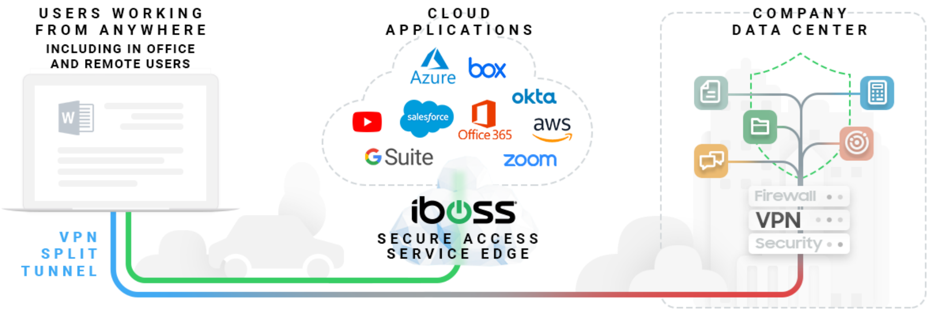
Bad

Sending all traffic through a VPN to a datacenter hosting proxy appliances is the worst case scenario and will lead to slow and unusable connections for users, especially remote workers.



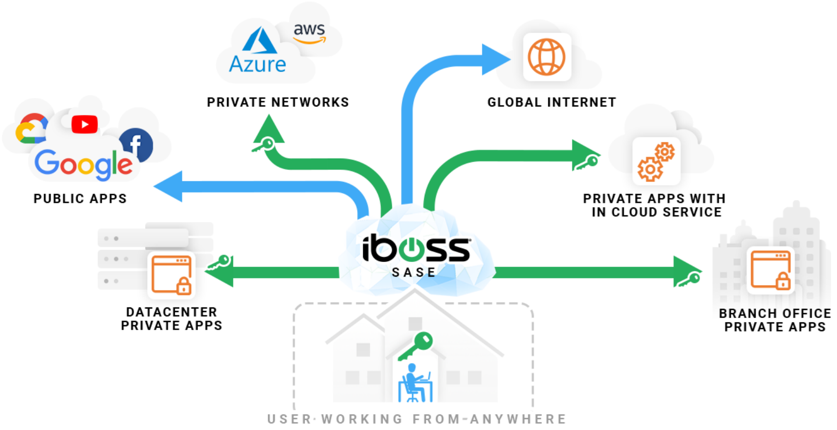
Better

Leverage iboss as your Secure Access Service Edge (SASE) platform for internet bound traffic. Offloading Internet bound traffic to iboss while only sending traffic that terminates at the office through the VPN will greatly improve the end user experience by increasing connection speeds dramatically. The iboss cloud connector takes the default route on the end user device and automatically redirects all non-private traffic through iboss cloud for security. This improves user productivity and streamlines connections to Office 365, Zoom, Teams, and other cloud applications. It also reduces the proxy and network security appliance footprint and the data center as all heavy traffic processing is performed within iboss cloud which has infinite scale.



Best

Leverage iboss as your Secure Access Service Edge (SASE) platform for ALL network traffic, both public and private, so that users are connected directly to any cloud resource quickly and securely. Sending all traffic through iboss cloud, both private and public, connects users to all cloud resources quickly and securely based on user identity and role. It eliminates costs by eliminating proxy and network security appliances hosted at the data center or office by performing security functions in the cloud and eliminating VPN infrastructure. Users connect to iboss cloud and all traffic to Office 365, cloud applications and video conference apps such as Zoom and Microsoft Teams is sent directly from the user to the cloud application with no extra hops to on-prem infrastructure. Since iboss is connected to all resources, public and private, it can connect users directly to those resources based on user role with speed and security while greatly reducing infrastructure costs, management costs and improving user productivity as they work with the network speed necessary to use cloud applications efficiently. The iboss platform is the premier SASE and Zero Trust platform that is the center piece of your cloud transformation.



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

CONTACT SUPPORT

Support Overview
Open a Ticket

North America Support:
877-742-6832 X3
support.na@ibosscloud.com

LATAM Support:
+52 (55) 41696270
support.latam@ibosscloud.com

EMEIA Support:
+44 (0) 203 7908289
support.emeia@ibosscloud.com

APAC Support:
+63 (45) 4571057
support.apac@ibosscloud.com

CONTACT SALES

Request Demo
Request Information

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