For Healthcare

Purpose Built for Zero Trust to Protect Healthcare from Breaches and Data Loss

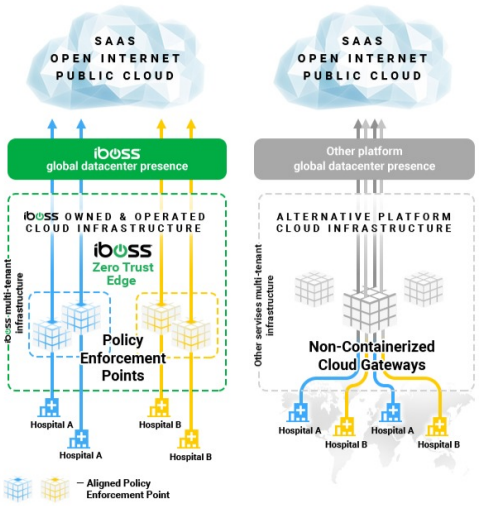
The iboss Zero Trust Edge prevents healthcare breaches by making applications, data and services inaccessible to attackers while allowing trusted users to securely and directly connect to protected resources from anywhere

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 Zero Trust Architecture ensures that any protected healthcare resource is inaccessible to attackers while allowing trusted users to securely and directly connect to those protected applications, services, or data from anywhere.

The iboss Zero Trust Edge is the leading Zero Trust cloud 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 full compliance with NIST SP 800-207 requirements. 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.

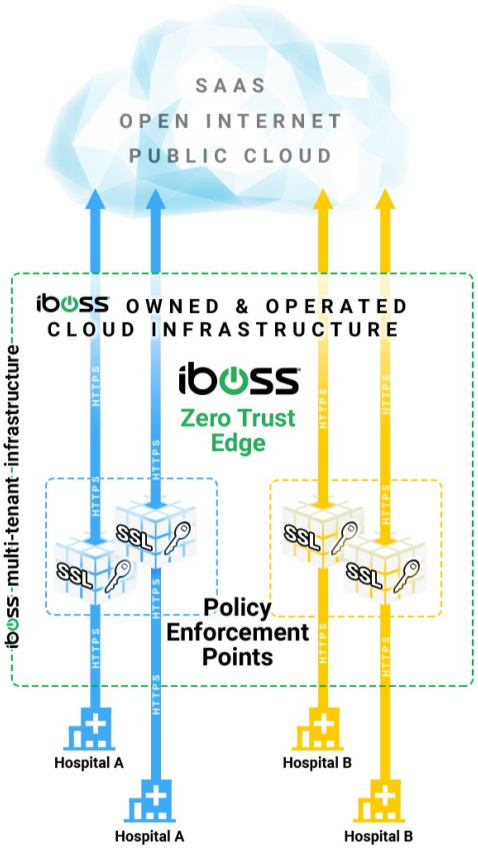
A Zero Trust Edge Security Service with Containerization at its Core

Understanding containerization is the key for healthcare institutions in need of a highly secure Zero Trust 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 Zero Trust solution.



With alternative Zero Trust platforms that lack containerization, network traffic from multiple organizations are processed within the same policy enforcement points (PEPs) that proxy, decrypt and firewall data for other organizations. Mixing data within the PEPs 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 Zero Trust 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.

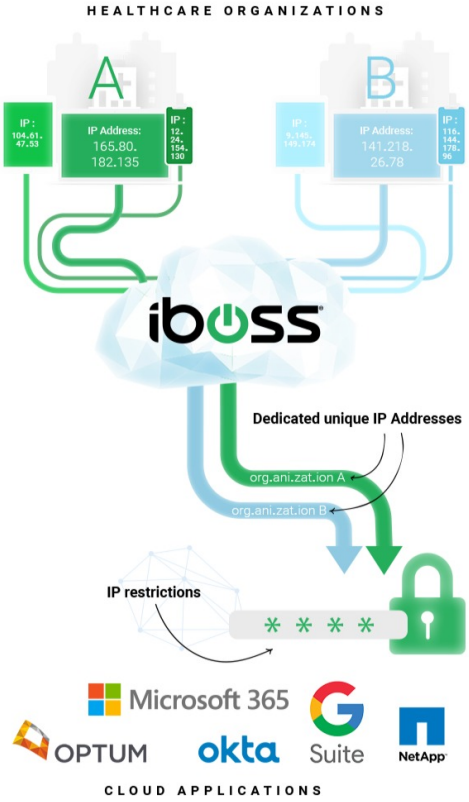
With a containerized cloud architecture like iboss, full isolation of data is achieved as it moves between users and the cloud, including full isolation of the private keys required to decrypt that traffic. The containerized cloud policy enforcement points isolate the private SSL decryption keys to ensure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

A Zero Trust Architecture Designed for Healthcare Institutions with Dedicated Source IP Addresses to minimize the policy enforcement point to protect Resources from attackers

Healthcare 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 healthcare 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 healthcare organizations' operated networks and untrusted remote networks. All traffic originating from users first traverses the iboss cloud policy enforcement point before making it to its final destination, including public cloud destinations and other destinations like Microsoft 365. And because the iboss platform is a cloud platform that is built on containerization, the source IP Address that is visible to the destination is always dedicated to the healthcare company. 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 healthcare company.



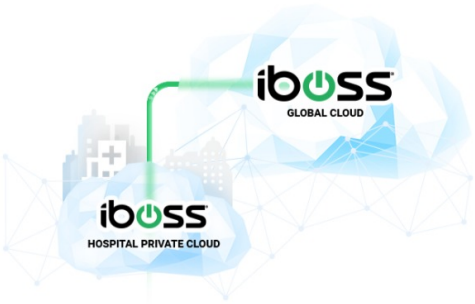
This has major advantages for healthcare organizations which are connecting users to trusted partners, vendors and IT platforms from locations outside of the traditional network perimeter. First, when a user connects to a cloud application service such as Microsoft 365, the company can guarantee that 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 healthcare institution.

Additionally, the dedicated and sticky IP Addresses provided by the iboss cloud 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 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 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 service between organizations are shared and although you can lock the cloud application down to the ranges belonging to the cloud service, you cannot guarantee the user accessing the front door of the application is an employee of the company. Any user running through the service, belonging to any account of the service, can access the application as the entire IP space of the 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.

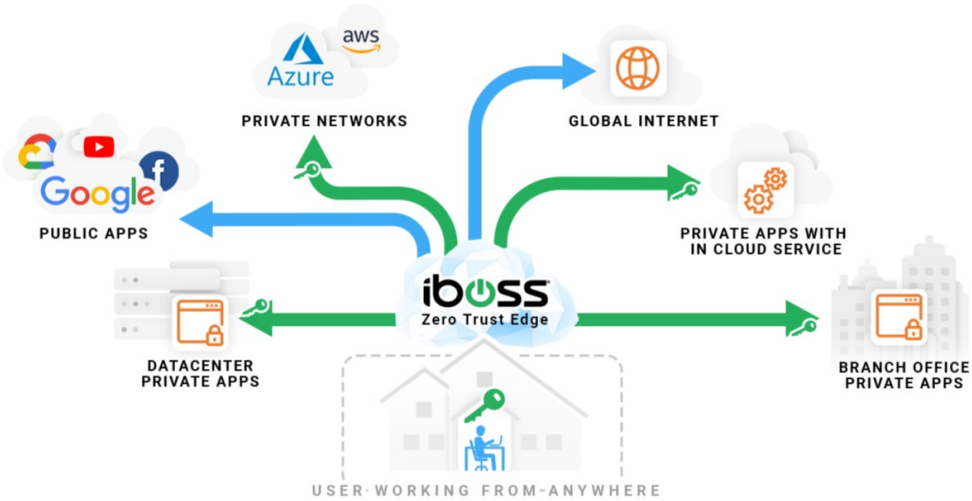
A Containerized Zero Trust Architecture that is Naturally Hybrid for Easy to Deploy Private Cloud



A containerized architecture allows the containerized cloud policy enforcement points (PEPs) to extend into physical form so they can be run within the company's network itself. This includes running the PEPs within an office or data center. The containerized PEPs 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 PEPs running within the service.

This is much different than alternative cloud services which are not based on containerization and do not have the ability to naturally extend into private cloud form. When the iboss Zero Trust cloud containerized policy enforcement points run onsite, within the company's network, they are linked to the global containerized cloud footprint. This means that traffic from remote users does not have to traverse back to the company 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 company datacenter. Deployments can be as many private cloud policy enforcement points and iboss cloud policy enforcement points as needed and can even shift over time. This provides the flexibility to transition from an on-prem private Zero Trust model to a full Zero Trust cloud model over time and with ease while gaining the benefits of protecting remote workers immediately today.

The Premier Zero Trust Edge



Take the next step in shifting to the world's largest security platform built for the future.

Sign up for a demo to see how the iboss Zero Trust Edge prevents breaches by making applications, data and services inaccessible to attackers while allowing trusted users to securely and directly connect to protected resources from anywhere.

REQUEST DEMO | CONTACT US | Corporate Data Sheet