Whitepaper

Why iboss cloud Beats Other Cloud Security Solutions

Transitioning internet security from web gateway appliances to the cloud is a requirement to meet the demands of the cloud-first future.

Exponential increases in bandwidth, expansive user mobility, and the shift of applications to the cloud has made securing user internet connectivity in the cloud an absolute must. iboss cloud shifts the focus from defending perimeters to following users to ensure internet access is secure regardless of location.

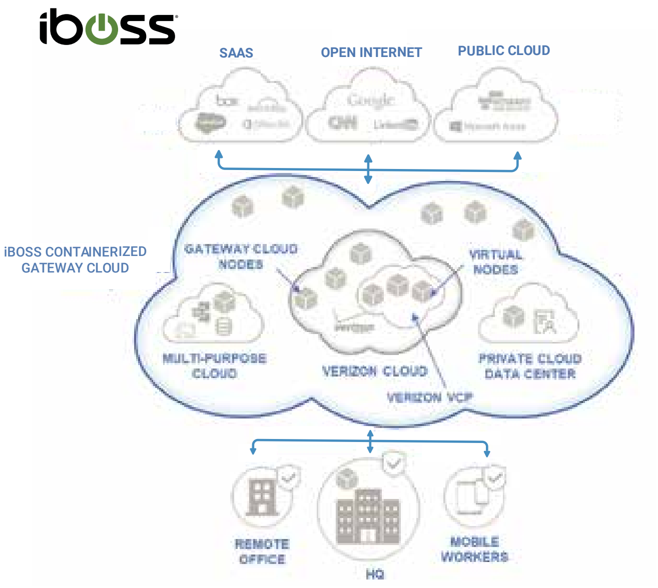
There's no question an on-prem web gateway appliance solution is unsustainable—the projected increases in bandwidth consumption combined with backhauled mobile traffic will quickly saturate the maximum capacity of any on-prem appliance architecture. The erosion of the network perimeter due to increased use of cloud apps and services further accelerates this backhauling, resulting in a poor end-user experience and lower productivity due to latency. Making the right choice when transitioning from an on-prem web appliance-based approach to a cloud solution is critical to ensure that no security capabilities are sacrificed—only the appliances themselves, and the headaches that come with them.

iboss: Containerized Cloud Architecture

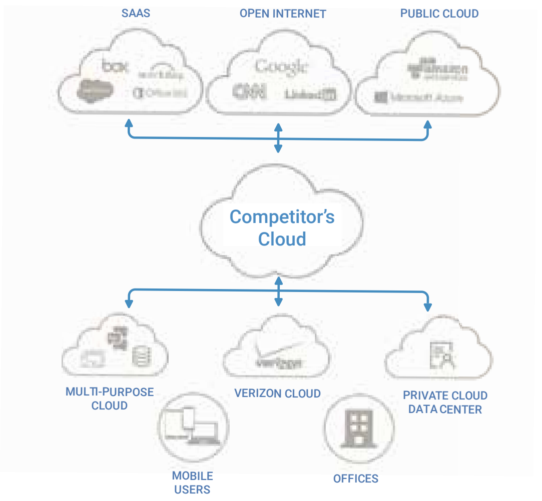
While both iboss cloud and competitors will migrate organizations from appliances to the cloud, only iboss can maintain all critical web gateway capabilities to ensure a seamless and frictionless transition. The following are just a few of many verifiable advantages that iboss cloud's containerized cloud architecture give it over other solutions:

> *"Only iboss cloud can maintain all critical web gateway capabilities to ensure a seamless and frictionless transition."*

1. User and group-based Terminal Server support in the cloud
2. 100% dedicated IP addresses in the cloud
3. Inspection of SSL traffic by default (does not require package upgrade)
4. Admin-defined cloud zones for data compliance
5. Intrusion Preventon for users outside the office network perimeter
6. Real-time log streaming to SIEM or logging databases directly from the cloud without the need for virtual appliances
7. Cloud SOCKS proxy support
8. Complex policy support including Policy Inheritance and Policy Layers

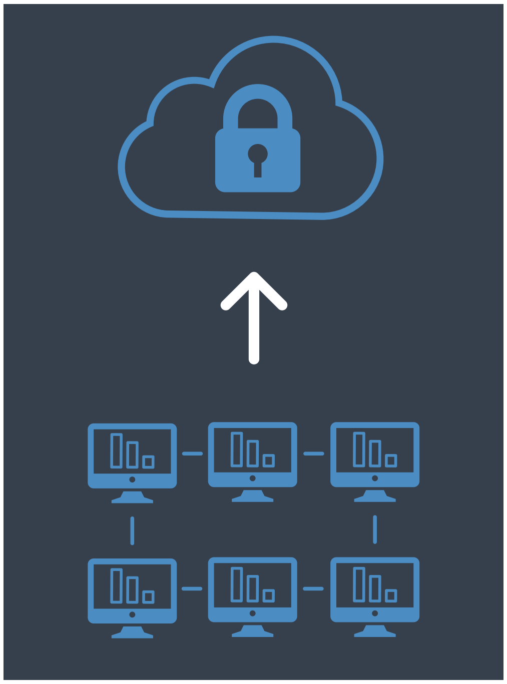


Competitor's Cloud Security Offering



User- and Group-based Terminal Server Support in the Cloud

Securing Windows Terminal Servers with user-and group-based policies is easily accomplished with on-prem solutions. Typically, Kerberos or NTLM is used to determine user identity in Terminal Server systems. Since Terminal Servers have multiple users logged in at the same time, Kerberos can differentiate users authenticating each connection. The challenge when moving to a cloud-based internet security platform is that Kerberos is typically used for local network authentication and although possible, doesn't transition easily to the cloud. iboss cloud includes a Terminal Server cloud connector to automatically connect Windows Terminal Server users to iboss. In addition, the connector extracts username and group to apply dynamic web security policies as well as associate user identities to log events. Installation is seamless and can be achieved within seconds, quickly solving the seemingly complex problem of migrating Terminal Server users to the cloud.



100% Dedicated IP Addresses in the Cloud

When securing a user with on-prem web gateways, the user's source IP is dedicated to the organization. This source IP can be used to restrict admin portals, for example via Okta, by using the source IP as a requirement for login. When transitioning to a cloud internet security solution, it may appear that the ability to maintain dedicated IP Addresses is not possible. The architecture of the iboss cloud, however, allows every customer to receive 100% dedicated IP addresses that can be used in the same way local IP Addresses are used. The difference is that iboss cloud follows users as they move in and out of the physical network perimeter, resulting in dedicated IP addresses for users regardless of location. This capability can be applied to require that users access business applications only through connections that are secured by the gateway, even when working outside of the office or on personal devices.

Inspect All Traffic Including SSL Traffic by Default

As crime takes root in the web, most sites and services have begun encrypting their communications with users, with SSL being the most common protocol used to do so. Google predicts SSL traffic will represent over 65% of all Internet traffic by year end 2018. This makes the abiility to inspect SSL traffic essential for effective internet security. Without doing so, a growing majority of an organization's traffic will go unsecured, allowing for malware or internal bad actors to exfiltrate corporate data unseen to the gateway.

As a critical but process-intensive task, SSL decryption can easily overburden a traditional security appliances attempting to achieve full SSL visibility into content and cloud app usage. iboss' infinitely scalable cloud architecture expands and contracts as needed, and each customer's resources are fully containerized—unlike alternative solutions, iboss cloud keeps each organizations' decryption keys completely isolated from others', and allows admins to determine exactly where these keys reside.

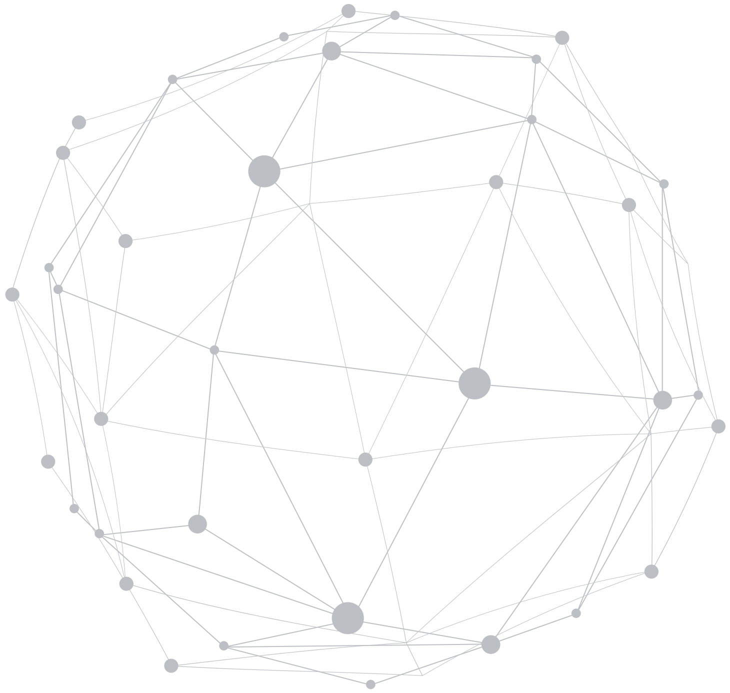
> ***"Because of the importance of SSL traffic inspection, iboss includes this feature by default with its core package."***

Moreover, iboss leverages patented technologies to provide flexibility to meet local and regulatory compliances, including the ability to define decryption rules based on geography. In contrast, other solutions may requires a package upgrade to achieve SSL traffic inspection, increasing the total cost of ownership of the solution. iboss understands that SSL is not an option, but a requirement for effective filtering.

Admin-defined Cloud Zones for Compliance

iboss cloud allows administrators to explicitly define cloud zones directly within the iboss cloud admin portal. These zones ensure users within a given region will be secured within the region and that log events generated within a given region to stay within the region. This is important for regulations such as GDPR, which require data to stay within national boundaries. Additionally, cloud zones can be used to define how users connect to iboss cloud, depending on location. For example, when users move from office to office, these admin-defined zones enable the dyamic bypassing of local printers and servers that apply to each office. The ability to create explicit zones is not present within competing platforms.

Follow the User Stream-Based Intrusion Prevention System



Stream-based intrusion prevention is easy to apply within network perimeters but extremely challenging when users travel outside that perimeter. This is because users move from place to place and work from networks outside of the control of the organization. When a user connects to the internet, the very first packet flows have no user identity and the source IP of their connections are only associated to the network they are originating from, such as a coffee shop's Wi-Fi. This lack of identifiable tags on the network stream makes it hard to distinguish one user from another. **iboss cloud is based on a containerized architecture which allows flow-based IP's to be applied to users wherever they roam.** This includes networks that are owned by the organization and networks that are not. A seemingly difficult impediment to migrating to a cloud-based security solution is easily solved by iboss cloud in a way that no other solution offers.

Real-time Streaming from the Cloud without Virtual Appliances

The need to stream log event data to external SIEMs or logging databases is a typical requirement for organizations. The SIEMs typically have processes built around them that are extensive and required. Since users are always connected to iboss cloud, regardless of location, their internet data is always secure and log events are continuously generated. Those log events are displayed in the included reporting dashboards of iboss cloud but can also be streamed in real-time to any external SIEM. While other platforms do offer services for streaming logs to SIEMs, they require virtual appliances to do so. These appliances must be installed and maintaned by the customer, creating more overhead for IT departments to manage.

The need to manage any hardware at all, however, is contradictory to the goals and benefits of transitioning to a cloud-based solution. With iboss cloud, such appliances are not necessary to stream logs concurrently in real-time to as many SIEMs as needed. For further control, iboss offers the ability to filter logs so that, for example, some SIEM teams receive only web logs while others receive malware or DLP logs.

Cloud SOCKS Proxy Support

In many on-prem web gateway proxy scenarios, a SOCKS proxy is required to allow applications to traverse to the cloud. The iboss cloud includes SOCKS proxy support to transition from on-prem web gateway proxies to the cloud with ease. As one major competitor states in its own material, it does not support the SOCKS protocol:

> **“SOCKS Proxy and SOCKS Proxy Port: You can leave these fields blank. [This solution] is NOT a SOCKS proxy. SOCKS traffic to ZENs are bypassed and allowed”**

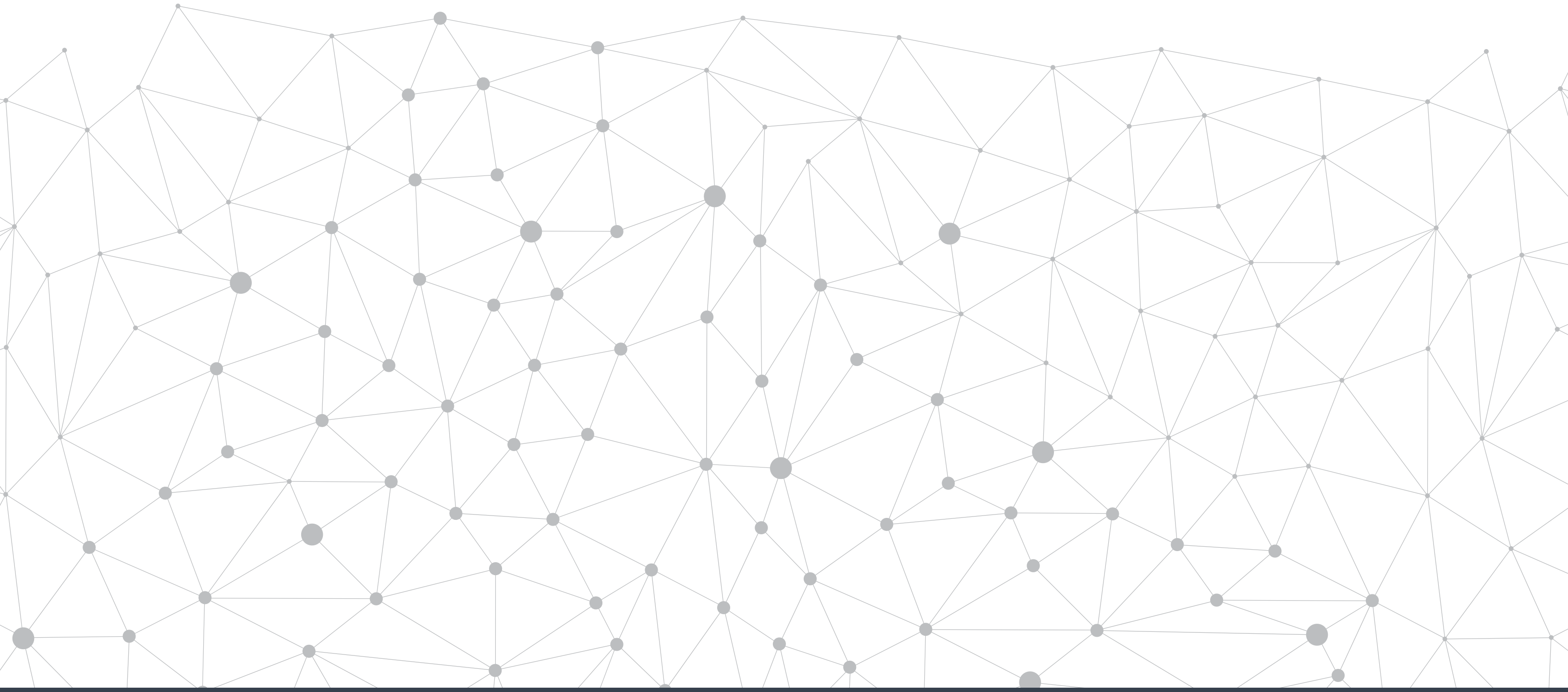
Again, iboss proves to be the more complete and flexible option.

Complex Policy Support, Including Policy Inheritance and Policy Layers

Transitioning years of policies that have been created on on-prem web gateway appliances may seem like a daunting task, assuming new the cloud-based solution even supports the features and capabilities needed to migrate of those policies. With iboss cloud, complex policies can easily be transitioned and capabilities such as Inheritance and Policy Layers can be used to recreate the complex policy sets. For example, Policy Inheritance allows for the creation of a base policy, to which more specific rules can be added. Policy Layers takes this a step further by allowing policies to be layered on top of the inherited policies to make an even more dynamic per-user policy possible. For example, regional restrictions may require blocking access to domains or destinations. A Policy Layer can be tied to particular networks and or groups so that the policy can be applied dynamically depending on environment. Competing products may not support Policy Inheritance or Layers, making it difficult to transition from on-prem security appliances to the cloud.

Summary

iboss cloud offers the most seamless transition from on-prem web gateway appliances to a cloud-based platform without sacrificing security or usability. The unique containerized architecture of iboss cloud eliminates the inefficiencies of on-prem appliance-based solutions and delivers full feature parity—and more—when compared with competing cloud security solutions.



About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances, which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture backed by 110 patents and over 100 points of presence globally, iboss protects more than 4,000 organizations worldwide.

To learn more, visit www.iboss.com

iboss, Inc.· U.S. HQ 101 Federal Street, 23rd Floor, Boston, MA 02110