For Business

iboss cloud DNS Protection for BYOD and Guest Network Protection

Included with the platform is the ability to protect networks by pointing DNS settings to the iboss cloud. This is a great choice for protecting guest and BYOD networks where devices are not owned by the organization but protection from Internet threats is still required.

Cloud DNS protection can easily be used to secure branch office locations without touching endpoints or re-configuring devices. The DNS settings of the network are changed to point to iboss cloud. When the iboss cloud receives a DNS query from the network, the query is run through the malware security stack to determine if the destination is malicious or the request represents malware command and control center traffic which indicates an infection.

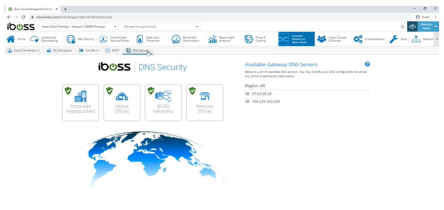
The use of DNS protection is powerful for BYOD networks where guests are able to leverage Wifi provided by the organization but the devices being used are not owned by the organization. Because the devices will automatically use the network-provided DNS settings, any query made by the BYOD device will be forwarded to iboss cloud for protection.

Easily configure guest network settings so that devices automatically receive protection

Web Filtering and Malware Protection with reporting

Unique policies can be applied to each guest network

Easily configure guest network settings so that devices automatically receive protection



The iboss cloud includes support for DNS-based protection in the cloud. This allows administrators to configure guest and BYOD networks to point to iboss cloud to extend web filtering and malware protection to devices not owned by the organization. Since the DNS settings of the BYOD network points to the iboss cloud, it will distribute the protection to any device connected to the network. The configuration is painless and requires no configuration on the devices connected to the network. The settings are automatically transferred via DHCP to the devices attached to guest network.

Web Filtering and Malware Protection with reporting

Web filtering policies can be applied to prevent risky Internet access for any device on the guest network. Malware protection automatically extends to any device connected to the network as well. Since DNS queries are directed to iboss cloud, the queries are automatically run through threat feeds and through policy engines. If violations occur, the user is presented with a customizable page indicating access was restricted.

Unique policies can be applied to each guest network

For each network configured for protection by iboss cloud, a unique default policy can be applied. This allows flexibility for different types of Wifi guest networks or offices. The guest or office network is mapped to the unique policy via its source IP and that policy is fully customizable by the network admin. This includes web filtering and malware controls.

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