

Replace McAfee with iboss

The Best McAfee Replacement



Proxy appliances were not designed for the modern, cloud-driven, world. They were designed to protect network traffic for users within offices, yet those users are working from home. They were designed to handle a predefined amount of network traffic, yet the volume of traffic is increasing exponentially by the day. Network proxy appliances were designed to decrypt and inspect limited amounts of encrypted HTTPS traffic. However, over 99% of all browsing time is over encrypted HTTPS connections according to the Google HTTPS Transparency Report. Proxy appliances were not designed for the cloud driven and mobile world. Switching to iboss ensures you get all of the network security capabilities found in proxy appliances, without the appliances and at infinite scale. This reduces infrastructure costs, reduces labor and is designed for the work from home and mobile future.

The iboss Platform is Designed for Mobile and Work from Anywhere Users

Users are not sitting behind the McAfee proxy appliances. They are working remotely, from home. If the network traffic does not traverse the McAfee appliances, it cannot inspect or protect that data. Because of this, organizations leveraging on-prem proxy appliances, like McAfee, are forced to send network data from remote users through slow VPN connections to provide network security. This is unsustainable and results in slow connections which reduces productivity and increases costs.

The iboss cloud platform provides all of the capabilities found in traditional and legacy McAfee appliances, except without the gear. It allows network data from remote users to be secured directly in the cloud, eliminating the unnecessary data backhaul through VPN connections. This results in fast connections, increased end-user productivity and reduced costs.



The iboss Platform Performs HTTPS Decryption at Scale

Over 99% of all browsing time is over encrypted HTTPS connections, according to the [Google HTTPS Transparency Report](#). Proxy appliances have compute and processing limitations and require a lot of hardware to handle the high volume of HTTPS traffic. This is extremely costly and typically results in extremely slow connections and the need to expand data center footprints.

The iboss cloud runs as a complete SaaS offering in the cloud. It has infinite computing power to decrypt any volume of traffic, without increasing costs. As encrypted traffic increases, your costs do not as iboss will process, decrypt and inspect all traffic automatically. This includes the large volumes of traffic from remote work from home users.



Cloud Applications Require More Bandwidth Which Is In Direct Conflict with Proxy Appliances

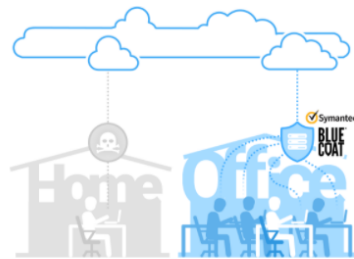
McAfee appliances are purchased to match the limited amount of bandwidth at the offices they are protecting. The problem is bandwidth is increasing by the day and more bandwidth is required to make employees productive while using cloud applications. As bandwidth increases, the proxy appliances will hit their maximum throughput causing more appliance purchases and management overhead.



The iboss cloud platform provides exactly the same capabilities and benefits instantly, while eliminating all of the overhead related to hosting and managing appliances. As bandwidth increases, the iboss cloud platform automatically handles the increases in load without creating additional burdens for the IT team or the company budget. It's all of the McAfee benefits, without all of the headaches.

McAfee Proxy Appliances Leave Cybersecurity Blindspots as Users Work From Anywhere

If the network traffic is not traversing the McAfee appliances, it cannot provide the protection or generate the log events that provide cybersecurity teams the visibility they need to enforce compliance, prevent malware and eliminate data loss. The appliances are only capable of inspecting traffic within the office.



With iboss cloud, all network traffic is always inspected before going to the cloud, regardless of user location. This includes protection for users in the office and those working from home. It can also generate the log events and drill down reports needed to ensure a strong cybersecurity posture for all users, from all locations, at all times. In addition, the iboss cloud can force network traffic to business applications while preventing traffic to personal cloud accounts, such as Google Drive. This reduces shadow IT and data loss from users, including those that work from home.

The iboss platform offers a 100% drop in replacement for McAfee proxy appliances converting a data center from simply hosting legacy proxy appliances to becoming a private cloud Point of Presence. The private cloud is linked to the global iboss cloud and immediately converts McAfee appliances to a modern private cloud extension of the iboss cloud global footprint.



The private cloud iboss appliances represent containerized cloud gateway capacity that can service on-prem users and devices with the exact same deployment and authentication model as the McAfee solution. For example, if the McAfee appliances use WCCP or ITD, the iboss private cloud capacity will support WCCP or ITD in the exact same way. If the on-prem McAfee deployment involves using F5 WIPs, the iboss containerized private cloud will support the F5 WIPs in exactly the same way without changing the network topology. If the McAfee appliances are deployed using explicit proxy, the iboss private cloud will take the place of the McAfee appliances and support the explicit proxy in the exact same way.

This makes transitioning to iboss from McAfee the easiest path on the market. In addition, since the private cloud is linked to the global iboss cloud footprint, all users outside of the private cloud network automatically send their traffic to iboss cloud. When the time comes, the private cloud is turned down and nothing changes for the organization as the private cloud was seen as just another data center within the global iboss cloud footprint.

Switch from McAfee to iboss

iboss Versus McAfee	iboss	McAfee
Complex and Robust Policy Engine	✓	✓
Designed For Users Working from Anywhere	✓	—
Greater Security With Firewall, IPS and Connection Tracking For Remote Users	✓	—
Scales Infinitely With Bandwidth Increases	✓	—
Can Decrypt Infinite Amounts of HTTPS Traffic in the Cloud	✓	—
Provides Reporting Visibility Natively for All Users	✓	—

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...

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

EMEA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

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

EMEA Support:
+44 (0) 203 7938289
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

EMEA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com



Copyright © 2020
iboss. All Rights Reserved.