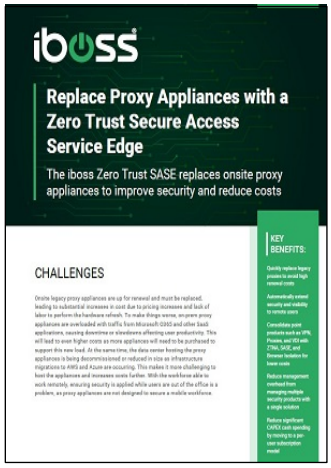


Replace Proxy Appliances with a Zero Trust Secure Access Service Edge

Solution Brief

Thank you for downloading this iboss solution brief. Carahsoft serves as iboss' Master Government Aggregator® making the company's cyber solutions and services available to the Public Sector through Carahsoft's network of reseller partners, Solutions for Enterprise-Wide Procurement (SEWP) V, Information Technology Enterprise Solutions – Software 2 (ITES-SW2), NASPO ValuePoint Cooperative Purchasing Contract, and other contract vehicles.

To learn how to take the next step toward acquiring iboss' solutions, please check out the following resources and information:

For additional resources:
carah.io/ibossResources

For upcoming events:
carah.io/ibossEvents

For additional iboss solutions:
carah.io/ibossSolutions

For additional iboss NetBackup solutions:
carah.io/ibossNetBackup

To set up a meeting:
iboss@Carahsoft.com
(703)-889-9710

To purchase, check out the contract vehicles available for procurement:
carah.io/ibossContracts

For more information, contact Carahsoft or our reseller partners:
iboss@carahsoft.com | (703)-889-9710

Replace Proxy Appliances with a Zero Trust Secure Access Service Edge

The iboss Zero Trust SASE replaces onsite proxy appliances to improve security and reduce costs

CHALLENGES

Onsite legacy proxy appliances are up for renewal and must be replaced, leading to substantial increases in cost due to pricing increases and lack of labor to perform the hardware refresh. To make things worse, on-prem proxy appliances are overloaded with traffic from Microsoft O365 and other SaaS applications, causing downtime or slowdowns affecting user productivity. This will lead to even higher costs as more appliances will need to be purchased to support this new load. At the same time, the data center hosting the proxy appliances is being decommissioned or reduced in size as infrastructure migrations to AWS and Azure are occurring. This makes it more challenging to host the appliances and increases costs further. With the workforce able to work remotely, ensuring security is applied while users are out of the office is a problem, as proxy appliances are not designed to secure a mobile workforce.

KEY BENEFITS:

- Quickly replace legacy proxies to avoid high renewal costs
- Automatically extend security and visibility to remote users
- Consolidate point products such as VPN, Proxies, and VDI with ZTNA, SASE, and Browser Isolation for lower costs
- Reduce management overhead from managing multiple security products with a single solution
- Reduce significant CAPEX cash spending by moving to a per-user subscription model

SOLUTION BRIEF

SOLUTION

The iboss Zero Trust Secure Access Service Edge is an advanced security solution that completely replaces the functionality delivered by legacy on-prem proxies with a global consolidated cloud security service. The iboss Zero Trust SASE includes ZTNA, CASB, malware defense, compliance policies, Browser Isolation, and logging that applies to users inside and outside the office. It scales to secure traffic volume as functionality is delivered within the cloud security service instead of only within appliances hosted within the data center. In addition, the iboss Zero Trust SASE can extend the Secure Access Service Edge into the data center by providing onsite gateways that are direct drop-in replacements to legacy proxies, such as Broadcom or McAfee Proxies, which allows local resources to be protected and a migration to occur with no network topology changes. This ensures a fast and smooth transition to iboss before the high-cost renewal date for the on-prem proxy arrives, resulting in substantial savings. Because the iboss Zero Trust SASE consolidates multiple point products into a single solution, costs are reduced even further. The iboss platform includes ZTNA to replace VPN, Secure Access Service Edge to replace legacy proxies, and Browser Isolation to replace legacy VDI. As the security technology stack gets consolidated and costs are reduced, users get better security and an improved end-user experience.

KEY BENEFITS:

- Quickly replace legacy proxies to avoid high renewal costs
- Automatically extend security and visibility to remote users
- Consolidate point products such as VPN, Proxies, and VDI with ZTNA, SASE, and Browser Isolation for lower costs
- Reduce management overhead from managing multiple security products with a single solution
- Reduce significant CAPEX cash spending by moving to a per-user subscription model

SOLUTION CAPABILITIES

Consolidates VPN, Proxies, and VDI into a single solution that includes ZTNA, Secure Access Service Edge, and Browser Isolation

Includes CASB, malware defense, DLP, Exact Data Match, compliance policies, and logging for users onsite and remote

Improves the end-user experience while increasing security by isolating access to resources

Provides secure and authenticated resource access to contractors through Browser Isolation which supports SSO

Can extend natively into the data center with iboss onsite gateways that protect local resources without needing to send traffic to the cloud security edge

Learn more
www.iboss.com

iboss
SOLUTION BRIEF

KEY SOLUTION CAPABILITIES:

- Consolidates VPN, Proxies, and VDI into a single solution that includes ZTNA, Secure Access Service Edge, and Browser Isolation
- Includes CASB, malware defense, DLP, Exact Data Match, compliance policies, and logging for users onsite and remote
- Improves the end-user experience while increasing security by isolating access to resources
- Provides secure and authenticated resource access to contractors through Browser Isolation which supports SSO
- Can extend natively into the data center with iboss onsite gateways that protect local resources without needing to send traffic to the cloud security edge

PAIN POINTS

Pain Point	iboss Solution
High Proxy Appliance Renewal Costs – Proxy appliances, such as Broadcom or McAfee, are up for renewal at increased prices	Replace Proxies with Secure Access Service Edge – The iboss Zero Trust SASE is an instant replacement for legacy proxies before renewals come due, resulting in substantial savings
Proxy appliances fail to protect remote users – As users work remotely, on-prem proxy appliances cannot protect their connections without forcing traffic back through the data center via a VPN which is slow and expensive	Protect Users Regardless of Location - The iboss Zero Trust SASE protects onsite and remote users equally, with remote users being connected directly through the iboss cloud security service for protection.
Microsoft O365 Traffic is Saturating Proxies – With increased Microsoft O365 and SaaS use, connection speeds have slowed to a crawl resulting in lost user productivity	Security Delivered at Scale without Slowdowns – The iboss Zero Trust SASE can secure any traffic volume with infinite processing capability available within the cloud security service. This increases user productivity and lowers costs.
Contractors need access to sensitive resources – Third-parties and contractors need controlled, secured and authenticated access to sensitive resources within the enterprise to prevent data loss and breaches.	Contractor Access is Provided Through Browser Isolation – Browser Isolation, the replacement for VDI, allows contractors to access resources through a pane-of-glass using SSO authentication while ensuring security and logging are in place for all transactions.

PAIN POINT

High Proxy Appliance Renewal Costs – Proxy appliances, such as Broadcom or McAfee, are up for renewal at increased prices

iboss SOLUTION

Replace Proxies with Secure Access Service Edge – The iboss Zero Trust SASE is an instant replacement for legacy proxies before renewals come due, resulting in substantial savings

Learn more
www.iboss.com

USE CASES / BUSINESS VALUE:

Use Case/Challenges	Solution Description	Benefits
Need to replace Broadcom/McAfee Proxies before renewal	The iboss Zero Trust SASE provides onsite gateways that are direct drop-in replacements for legacy proxies with the same capabilities.	Quickly avoid high renewal costs and modernize security and connectivity during the process. Remote users will get the same security as onsite users because the onsite gateways extend the cloud security edge and support the same capabilities.
Need to secure remote workers	The iboss Zero Trust SASE is a cloud security service that allows remote workers to connect directly to cloud applications without the need for a VPN while ensuring security and visibility are in place.	Reduces the high costs associated with sending large volumes of traffic through the VPN, the unnecessary bandwidth overhead on data centers, and improves user security and productivity from faster connections.
Need to avoid buying more legacy proxies due to Microsoft O365 use which requires more capacity	The iboss Zero Trust SASE provides the same capabilities as legacy proxy appliances but scales horizontally to support any traffic volume.	Substantially reduce costs related to high-priced proxy appliances by leveraging the iboss Zero Trust SASE to handle the security and logging load in the cloud.
Need to reduce or eliminate data center space and have no place for legacy proxy appliances	The iboss Zero Trust SASE provides the same capabilities as the on-prem proxies but delivers those functions in the cloud. The iboss cloud service can also be connected directly to existing data centers through cross-connects or direct links to offload the resources needed within the data center to support the on-prem proxy appliances.	Significantly reduce costs and achieve cloud transformation by migrating legacy proxy appliances from self-hosted within the data center to a cloud-delivered service that has the same capabilities at scale.
Need to allow contractors and third parties access to sensitive resources	The iboss Zero Trust SASE provides third-party access through Browser Isolation which supports SSO via Azure, Okta, Ping, or any SAML capable Identity Provider. Isolated sessions are VDI-like, prevent data from touching third-party devices, and only provide access to authorized resources.	Reduce or eliminate the cost of expensive infrastructure related to VDI and replace it with instant Browser Isolation delivered by the iboss Zero Trust SASE. Browser Isolation is available globally and can connect users in any region without infrastructure costs.

PAIN POINT

Proxy appliances fail to protect remote users – As users work remotely, on-prem proxy appliances cannot protect their connections without forcing traffic back through the data center via a VPN which is slow and expensive

iboss SOLUTION

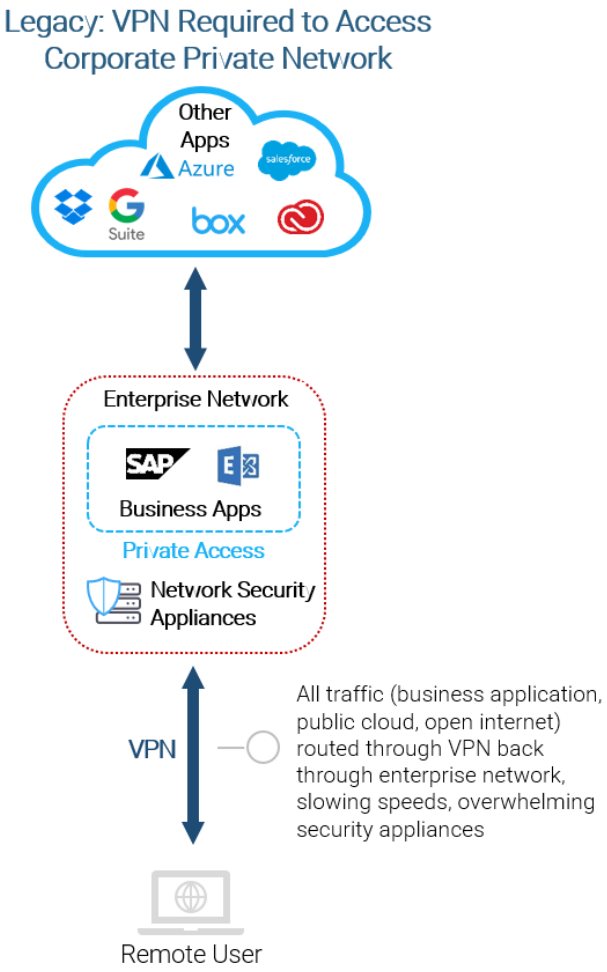
Protect Users Regardless of Location - The iboss Zero Trust SASE protects onsite and remote users equally, with remote users being connected directly through the iboss cloud security service for protection.

Learn more
www.iboss.com

iboss
SOLUTION BRIEF

TECHNICAL SOLUTION:

Legacy proxies are typically installed at data centers or core offices to protect organizations from malware and data loss and apply compliance. Proxy appliances have limited capacity and are designed to protect onsite users. Remote users suffer from slow connections that are backhauled via VPN through the hosted proxy appliances, resulting in substantial lost productivity and a poor end-user experience. In addition, the high renewal costs for proxy appliances increase upfront cash spending, which worsens if more appliances are purchased to handle increased traffic loads.



The iboss Zero Trust SASE can solve those problems by quickly replacing on-prem proxies, such as Broadcom and McAfee appliances, with a cloud-delivered Secure Access Service Edge. The iboss service includes CASB, malware defense, DLP, Exact Data Match, compliance policies, HTTPS decrypt and logging at scale and delivered in the cloud.

PAIN POINT

Microsoft O365 Traffic is Saturating Proxies – With increased Microsoft O365 and SaaS use, connection speeds have slowed to a crawl resulting in lost user productivity

iboss SOLUTION

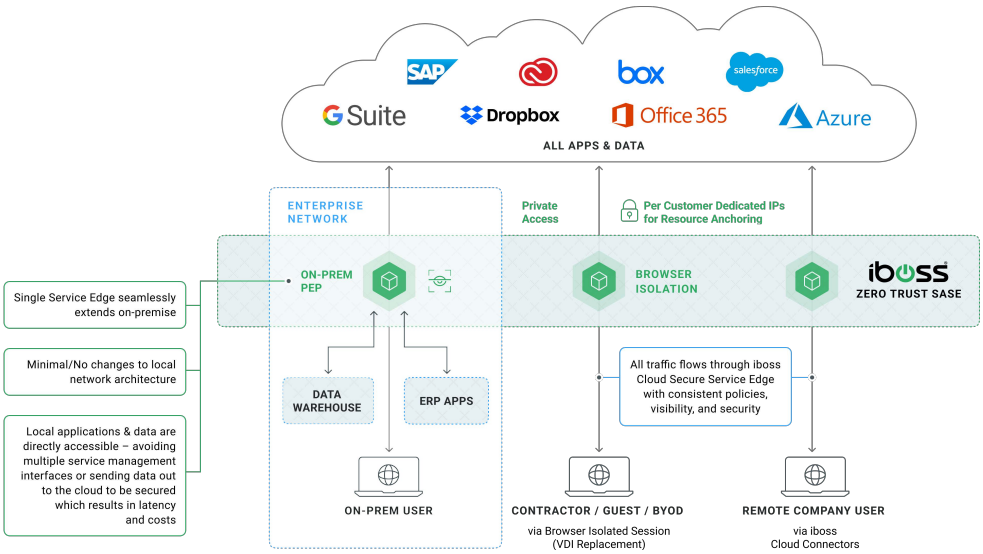
Security Delivered at Scale without Slowdowns – The iboss Zero Trust SASE can secure any traffic volume with infinite processing capability available within the cloud security service. This increases user productivity and lowers costs.

Learn more
www.iboss.com

SOLUTION BRIEF

iboss' Zero Trust Secure Access Service Edge

A Single Unified Edge - Eliminating VPNs, VDIs, & Legacy On-Prem Proxies



The iboss Zero Trust SASE is built from a containerized architecture which allows the Policy Enforcement Points, or gateways, to be deployed within the data center. These gateways extend the same security and logging capabilities within the cloud secure access service edge locally to the data center without sending traffic to the cloud security service first when accessing local resources. This allows fast migrations from legacy proxies while providing the fastest, most optimal connections for onsite users accessing local resources.

The iboss Zero Trust SASE provides extensive network and security capabilities that completely replace VPN, Proxies, and VDI with ZTNA, Secure Access Service Edge, and Browser Isolation. This increases security, improves the end-user experience, consolidates technology, and substantially reduces costs.

PAIN POINT

Contractors need access to sensitive resources – Third parties and contractors need controlled, secured, and authenticated access to sensitive resources within the enterprise to prevent data loss and breaches.

iboss SOLUTION

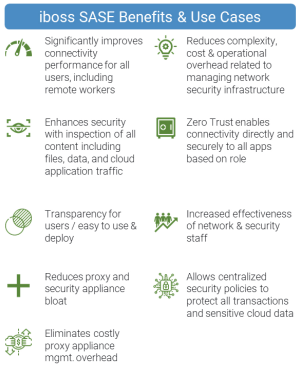
Contractor Access is Provided Through Browser Isolation – Browser Isolation, the replacement for VDI, allows contractors to access resources through a pane-of-glass using SSO authentication while ensuring security and logging are in place for all transactions.

Learn more
www.iboss.com

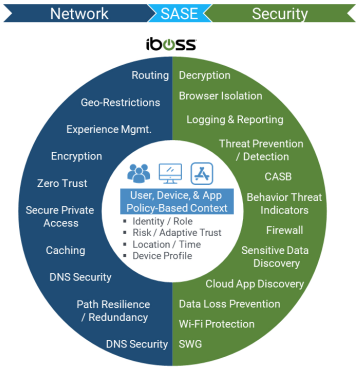
SOLUTION BRIEF

A Complete Platform: ZTNA + Secure Access Service Edge

Providing both Connectivity and Advanced SaaS Security Services



iboss Zero Trust Security Service Edge



ABOUT IBOSS

iboss is a cloud security company that enables organizations to reduce cyber risk by delivering a Zero Trust Secure Access Service Edge platform designed to protect resources and users in the modern distributed world. Applications, data and services have moved to the cloud and are located everywhere while users needing access to those resources are working from anywhere. The iboss platform replaces legacy VPN, Proxies and VDI with a consolidated service that improves security, increases the end user experience, consolidates technology and substantially reduces costs. Built on a containerized cloud architecture, iboss delivers security capabilities such as SWG, malware defense, Browser Isolation, CASB and Data Loss Prevention to protect all resources, via the cloud, instantaneously and at scale. The iboss platform includes ZTNA to replace legacy VPN, Secure Access Service Edge to replace legacy Proxies and Browser Isolation to replace legacy VDI. This shifts the focus from protecting buildings to protecting people and resources wherever they are located. Leveraging a purpose-built cloud architecture backed by 230+ issued and pending patents and more than 100 points of presence globally, iboss processes over 150 billion transactions daily, blocking 4 billion threats per day. More than 4,000 global enterprises trust the iboss platform to support their modern workforces, including a large number of Fortune 50 companies. iboss was named one of the Top 25 Cybersecurity Companies by The Software Report, one of the 25 highest-rated Private Cloud Computing Companies to work for by Battery Ventures, and CRN's top 20 Coolest Cloud Security Companies of 2022.

To learn more, visit **www.iboss.com**.

KEY BENEFITS:

Quickly replace legacy proxies to avoid high renewal costs

Automatically extend security and visibility to remote users

Consolidate point products such as VPN, Proxies, and VDI with ZTNA, SASE, and Browser Isolation for lower costs

Reduce management overhead from managing multiple security products with a single solution

Reduce significant CAPEX cash spending by moving to a per-user subscription model

Learn more
www.iboss.com