Replace VPN, Proxy, and VDI with iboss Zero Trust SASE

Replace legacy VPN, Proxy, and VDI with ZTNA, Secure Access Service Edge, and Browser Isolation with a Single Platform

CHALLENGES

Multiple point security point products are leading to high complexity and costs. VPNs are necessary to connect remote users to private resources but are slow, cumbersome, and result in a poor end-user experience. 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. VDI provides isolated access to contractors, guests, and call center agents but is expensive due to the infrastructure and data center space needed to operate it. On-prem proxy appliances and VPNs are overloaded with traffic from Microsoft O365 and other SaaS applications, causing downtime or slowdowns affecting user productivity. The data center is also slated to be turned down or substantially reduced as technology moves to AWS and Azure, leaving no place for the VPN concentrators, proxies, or VDI infrastructure. To make things worse, CAPEX and OPEX must be reduced quickly, including large cash expenditures, which the finance team has mandated.

KEY BENEFITS:

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

Connect remote workers to onsite resources without a VPN using ZTNA

Automatically extend security and visibility to remote users without Proxy appliances using a Secure Access Service Edge

Provide isolated access to contractors, guests, and call center users without VDI by using Browser Isolation

SOLUTION BRIEF

SOLUTION

The iboss Zero Trust SASE replaces legacy VPN, Proxies, and VDI with a consolidated service that improves security, increases the end-user experience, consolidates technology, and substantially reduces costs. The iboss platform includes ZTNA to replace legacy VPN, Secure Access Service Edge to replace legacy Proxies, and Browser Isolation to replace legacy VDI. The iboss Zero Trust Secure Access Service Edge is an advanced security solution that completely replaces the functionality delivered by legacy security point products with a global consolidated cloud security service.

The iboss Zero Trust SASE includes ZTNA, CASB, malware defense, compliance policies, DLP, 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 strictly with appliances hosted within the data center. VPN can be replaced with ZTNA, which provides better security and runs in the background to connect users to private applications and data automatically. Legacy proxy appliances, such as those from Broadcom and McAfee, can be replaced with Secure Access Service Edge, which extends security to all users, including remote workers, by delivering capabilities in the cloud. VDI can be replaced with Browser Isolation which performs the same function of isolating access to applications and data but does not require infrastructure or data center space as it is streamed from the cloud and available globally.

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 which allow 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. As the security technology stack gets consolidated and costs are reduced, users get better security and an improved end-user experience.

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

Force SSO and MFA to all applications and services, even to legacy apps that do not support SAML

Performs automatic application and service discovery to identify risk from shadow IT and includes a resource catalog to identify and classify risk within the organization

Learn more
www.iboss.com

SOLUTION BRIEF

KEY BENEFITS:

- Consolidate point products such as VPN, Proxies, and VDI with ZTNA, SASE, and Browser Isolation for lower costs
- Connect remote workers to onsite resources without a VPN using ZTNA
- Automatically extend security and visibility to remote users without Proxy appliances using a Secure Access Service Edge
- Provide isolated access to contractors, guests, and call center users without VDI by using Browser Isolation
- Reduce risk and meet compliance by forcing SSO and MFA to all apps and services, including legacy resources that do not natively support it
- Prevent damage from infected devices by cutting access to sensitive resources automatically and without human intervention
- Identify and catalog all sensitive applications, data, and services to understand and reduce risk
- Reduce significant CAPEX cash spending by moving to a per-user subscription model

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

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
- Force SSO and MFA to all applications and services, even to legacy apps that do not support SAML
- Performs automatic application and service discovery to identify risk from shadow IT and includes a resource catalog to identify and classify risk within the organization

PAIN POINT

VPNs are slow, insecure, and cumbersome – Remote users need VPNs to access private resources, but they are impacting productivity and increasing organizational risk

iboss SOLUTION

Replace VPN with ZTNA – The iboss Zero Trust SASE includes ZTNA, which connects users only to authorized applications from any location to reduce risk and improve the end-user experience

Learn more
www.iboss.com

iboss
SOLUTION BRIEF

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
VPNs are slow, insecure, and cumbersome – Remote users need VPNs to access private resources, but they are impacting productivity and increasing organizational risk	Replace VPN with ZTNA – The iboss Zero Trust SASE includes ZTNA, which connects users only to authorized applications from any location to reduce risk and improve the end-user experience
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
Call Centers need isolated access to support applications – GDPR compliance and customer data risk requires support agents to be isolated from data	Browser Isolation Replaced VDI – Browser Isolation provides controlled and isolated access through a pane of glass to Call Center agents
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.
Security & Visibility Needed for Remote Workers – Onsite security appliances struggle to secure the remote workforce	Secure Access Service Edge Secures All Workers – With iboss, all workers have security and logging applied regardless of location, with security delivered in the cloud

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

Learn more
www.iboss.com

SOLUTION BRIEF

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, supporting the same capabilities.
Need to connect remote workers to onsite and private resources	The iboss Zero Trust SASE includes ZTNA, which connects remote workers to onsite and private resources automatically without ever enabling a VPN	ZTNA is more secure as it allows remote workers to access authorized applications instead of the entire enterprise network. ZTNA also runs in the background, so users can connect without turning on a VPN.
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 needing 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 and VPN concentrators due to Microsoft O365 use which requires more capacity	The iboss Zero Trust SASE provides the same capabilities as legacy proxy appliances and VPNs but scales horizontally to support any traffic volume.	Substantially reduce costs related to high-priced proxy appliances and VPN concentrators by leveraging the iboss Zero Trust SASE to handle the connectivity, security, and logging load in the cloud.
Need to reduce or eliminate data center space and have no place for legacy VPN concentrators, proxy appliances, or VDI infrastructure	The iboss Zero Trust SASE provides the same capabilities as VPN, proxies, and VDI 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 VPN, proxy appliances, and VDI from self-hosted within the data center to a cloud-delivered service with the same capabilities at scale.

PAIN POINT

Call Centers need isolated access to support applications – GDPR compliance and customer data risk requires support agents to be isolated from data

iboss SOLUTION

Browser Isolation Replaced VDI – Browser Isolation provides controlled and isolated access through a pane of glass to Call Center agents

Learn more
www.iboss.com

SOLUTION BRIEF

Use Case/Challenges	Solution Description	Benefits
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.
Need to replace VDI used at Call Centers to reduce costs	The iboss Zero Trust SASE eliminates VDI with Browser Isolation which performs the same function but does not require infrastructure and is available in all regions instantly.	Reduces infrastructure and operating costs related to VDI. Increases security by applying security and logging to interactions within the Browser Isolation session.

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

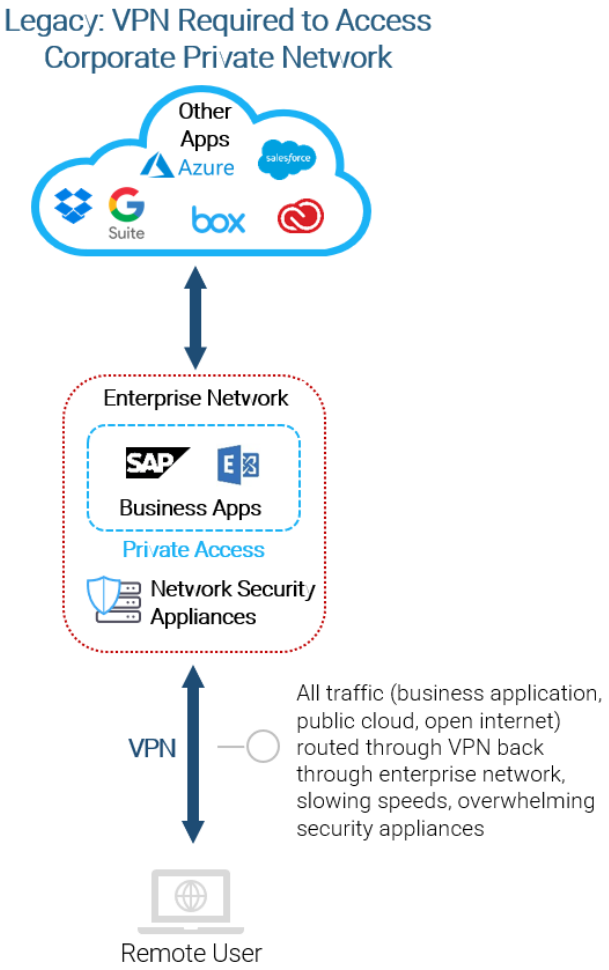
Protect Users Regardless of Location - The iboss Zero Trust SASE protects onsite and remote users equally, with remote users being connected directly through the iboss cloud security service for protection.

Learn more
www.iboss.com

SOLUTION BRIEF

TECHNICAL SOLUTION:

Legacy VPNs are slow and insecure but are required for remote workers. Legacy proxies are typically installed at data centers or core offices to protect organizations from malware and data loss and apply compliance. VDI is needed for contractors, guests, and Call Center agents to provide isolated access through a pane-of-glass when there is a risk of data leaking to high-risk or untrusted devices. Unfortunately, proxy appliances have limited capacity and are designed to protect onsite users. Remote users suffer from slow connections backhauled via VPN through the hosted proxy appliances, resulting in substantial lost productivity and a poor end-user experience. VDI requires expensive infrastructure, subscriptions, and data center hosting costs. In addition, the high renewal costs for VPNs, proxies, and VDI increases 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 legacy VPN, proxies, and VDI with a cloud-delivered Secure Access Service Edge. The iboss service includes ZTNA, CASB, malware defense, DLP, Browser Isolation, 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

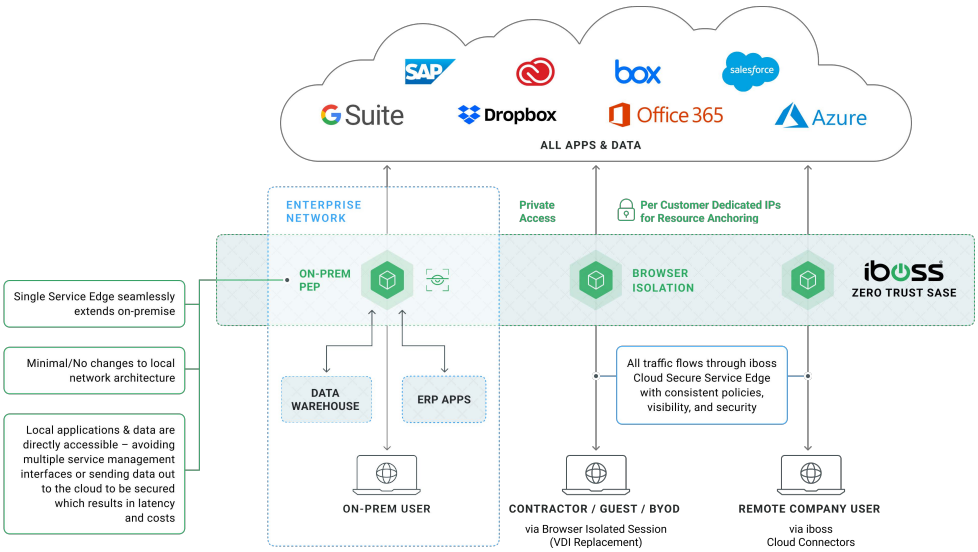
Security Delivered at Scale without Slowdowns – The iboss Zero Trust SASE can secure any traffic volume with infinite processing capability available within the cloud security service. This increases user productivity and lowers costs.

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 security service edge locally to the data center without needing to send 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

Security & Visibility Needed for Remote Workers – Onsite security appliances struggle to secure the remote workforce

iboss SOLUTION

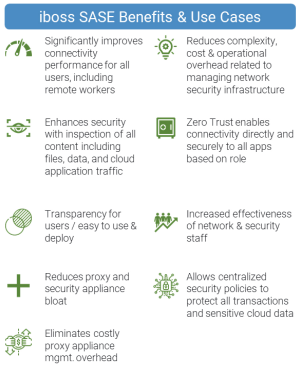
Secure Access Service Edge Secures All Workers – With iboss, all workers have security and logging applied regardless of location, with security delivered in the cloud

Learn more
www.iboss.com

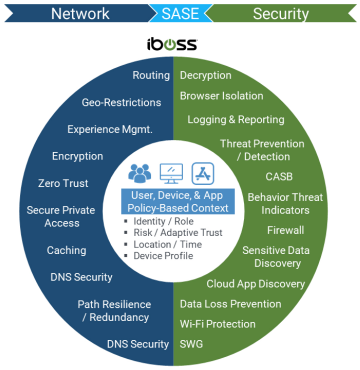
SOLUTION BRIEF

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:

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

Connect remote workers to onsite resources without a VPN using ZTNA

Automatically extend security and visibility to remote users without Proxy appliances using a Secure Access Service Edge

Provide isolated access to contractors, guests, and call center users without VDI by using Browser Isolation

Reduce risk and meet compliance by forcing SSO and MFA to all apps and services, including legacy resources that do not natively support it

Prevent damage from infected devices by cutting access to sensitive resources automatically and without human intervention

Identify and catalog all sensitive applications, data, and services to understand and reduce risk

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

Learn more
www.iboss.com