SOLUTION BRIEF

Replace VPN with ZTNA

The iboss Zero Trust SSE replaces VPN with ZTNA to improve security and reduce costs

CHALLENGES

Legacy VPNs provide access to resources for remote workers but do not provide tight controls on what resources can be accessed while users are connected. Once a user is connected to the VPN, they have free access to any resource available on the private network. As users interact with resources, no security is applied, such as CASB, malware defense, and Data Loss Prevention, leading to a significant risk of breach and data loss. Because transactions are not inspected, no logging visibility is provided to security teams to detect unauthorized access or data hijacking. To make things worse, the increased number of security point solutions requires different products for VPN, Proxies, and VDI, which are necessary to meet a minimum level of security acceptable to the organization. This increases management overhead and substantially increases costs.

KEY BENEFITS:

Quickly replace VPN to improve security by providing access on a per-application basis

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

Achieve higher security with continuous adaptive access that evaluates every request for security and compliance

Force MFA and SSO for all applications and services, including legacy applications that do not support SAML

SOLUTION

The iboss Zero Trust Security Service Edge is an advanced security solution that completely replaces the functionality delivered by legacy VPNs with a global consolidated cloud security service. The iboss Zero Trust SSE includes ZTNA, CASB, malware defense, compliance policies, Browser Isolation, and logging that applies to users inside and outside the office. The ZTNA capability connects remote users to onsite resources, completely replacing the need for VPN and eliminating the VPN budget line item. ZTNA is substantially more secure than VPN because it only allows remote users to access approved applications while automatically denying access to all other resources in the office. ZTNA also authenticates users with modern SSO, including MFA, and provides continuous authorization so that every access to sensitive resources is inspected for protection. If a device becomes infected, the user is cut from sensitive resources immediately. In addition, ZTNA connections run through the entire iboss Security Service Edge security stack, which means that CASB, malware defense, DLP, and logging will be applied to each connection. This provides the needed visibility to avoid data theft and the controls required to provide in-app controls to prevent breaches. The ZTNA service is delivered through iboss and does not require VPN concentrator appliances, eliminating CAPEX spending and management overhead. And because the iboss Zero Trust SSE consolidates multiple point products into a single solution, costs are reduced even further. The iboss platform includes ZTNA to replace VPN, Security 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 VPN to improve security by providing access on a per-application basis
- Consolidate point products such as VPN, Proxies, and VDI with ZTNA, SSE, and Browser Isolation for lower costs
- Achieve higher security with continuous adaptive access that evaluates every request for security and compliance
- Force MFA and SSO for all applications and services, including legacy applications that do not support SAML
- Gain visibility from detailed logging for every interaction between users and sensitive private resources
- Ensure devices are compliant before accessing sensitive resources, such as ensuring the device firewall is on, antimalware is running, and the disk is encrypted

SOLUTION CAPABILITIES

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

Includes CASB, malware defense, DLP, Exact Data Match, compliance policies, and logging for all interactions with sensitive private resources

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

Provides SSO and MFA for all types of resource access, including legacy apps, even when those apps do not support SAML or SSO

Performs device posture checks, such as ensuring antimalware is running, the firewall is on, and the disk is encrypted, before allowing access to sensitive resources

Learn more
www.iboss.com

KEY SOLUTION CAPABILITIES:

- Consolidates VPN, Proxies, and VDI into a single solution that includes ZTNA, Security Service Edge, and Browser Isolation
- Includes CASB, malware defense, DLP, Exact Data Match, compliance policies, and logging for all interactions with sensitive private resources
- Improves the end-user experience while increasing security by isolating access to resources
- Provides SSO and MFA for all types of resource access, including legacy apps, even when those apps do not support SAML or SSO
- Performs device posture checks, such as ensuring antimalware is running, the firewall is on, and the disk is encrypted, before allowing access to sensitive resources

PAIN POINTS

Pain Point	iboss Solution
VPNs are cumbersome for remote users – When users are remote, they must remember to turn on the VPN to access private or onsite resources.	Replace VPN with ZTNA – The iboss Zero Trust SSE is an instant replacement for legacy VPN and improves the end-user experience because it runs transparently and automatically with no end-user intervention
VPNs are slow and reduce productivity – VPNs are slow because they are saturated with unnecessary traffic being backhauled to be secured at the data center resulting in lost productivity.	ZTNA + Security Service Edge Provides Fast Access - The iboss Zero Trust SSE provides direct access to all applications without the need to traverse a VPN by delivering security in the cloud. This dramatically increases connection speeds and productivity.
VPNs provide too much access to onsite resources – VPNs cannot provide granular access controls and allow users to access any resource in the office when connected, which increases risk	ZTNA provides granular access controls – The iboss Zero Trust SSE provides per-app access controls and automatically denies all other resources. It also provides a complete security stack and logging to reduce risk and increase compliance.
Contractors need access to sensitive resources – Third parties and contractors need controlled, secured, and authenticated access to sensitive resources within the enterprise but must install a VPN to obtain it.	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, all without software or a VPN.

PAIN POINT

VPNs are cumbersome for remote users – When users are remote, they must remember to turn on the VPN to access private or onsite resources.

iboss SOLUTION

Replace VPN with ZTNA – The iboss Zero Trust SSE is an instant replacement for legacy VPN and improves the end-user experience because it runs transparently and automatically with no end-user intervention

Learn more
www.iboss.com

USE CASES / BUSINESS VALUE:

Use Case/Challenges	Solution Description	Benefits
Need to replace legacy VPNs such as Cisco Anyconnect	The iboss Zero Trust SSE provides ZTNA that eliminates VPN and improves security	Quickly replace VPN with ZTNA to reduce costs, increase security and improve the end-user experience.
Need to provide remote users access to onsite resources	The iboss Zero Trust SSE includes ZTNA that connects users to all resources, including those on-site, from wherever they work.	Eliminates point product solutions, such as VPNs, that only perform one function but consume a separate budget line item. This reduces costs and complexity and allows users to connect to whatever they need to do their most productive work.
Microsoft O365 traffic has saturated the VPN resulting in slow connections	As a Microsoft Certified Network and Security Partner, the iboss Zero Trust SSE offloads Microsoft O365 traffic and secures the connections directly within the cloud service. The cloud security service enforces Microsoft Tenant Restrictions eliminating the need for traffic backhaul to the data center.	Increased productivity, fewer complaints related to connectivity, and lower costs when implementing Microsoft Tenant Restrictions which are traditionally enforced in the data center using expensive proxy appliances.
Need to enforce device posture checks before allowing access to sensitive resources for security and compliance	The iboss Zero Trust SSE provides extensive device posture checks that include antimalware, firewall, and disk encryption checks and ensures compliance requirements are met before granting access to sensitive resources.	Dramatically reduces risk and ensures compliance is met without complicated management and configuration overhead.
Need to allow contractors and third parties access to sensitive resources without the need for a VPN	The iboss Zero Trust SSE 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. Browser Isolation eliminates the need for third parties to install VPN software as access is granted through a browser.	Reduce or eliminate the cost of expensive infrastructure related to VDI and replace it with instant Browser Isolation delivered by the iboss Zero Trust SSE. Prevent data from leaking to untrusted devices. Connect contractors without VPN software installs.

PAIN POINT

VPNs are slow and reduce productivity – VPNs are slow because they are saturated with unnecessary traffic being backhauled to be secured at the data center resulting in lost productivity.

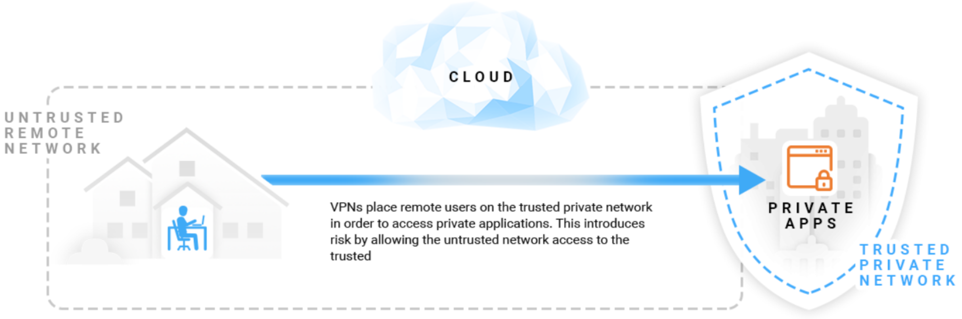
iboss SOLUTION

ZTNA + Security Service Edge Provides Fast Access - The iboss Zero Trust SSE provides direct access to all applications without the need to traverse a VPN by delivering security in the cloud. This dramatically increases connection speeds and productivity.

Learn more
www.iboss.com

TECHNICAL SOLUTION:

VPNs are used to connect remote workers to sensitive onsite resources. When connected, those users have access to anything on the remote network. This increases the risk of breach and data loss as users can access unauthorized resources. If those devices become infected, they can cause damage to data and critical business applications. In addition, the remote user's network, which may be infected, is connected to the private enterprise network, further increasing the risk of breach.



VPNs place remote users on the trusted private network in order to access private applications. This introduces risk by allowing the untrusted network access to the trusted

With VPNs, remote users are connected from their untrusted network to the trusted network to gain access to private apps

The iboss Zero Trust SSE can solve the issues related to VPN by replacing VPN with iboss ZTNA. ZTNA is a technology that increases security by only allowing users to access authorized resources while automatically denying access to everything else. In addition, VPNs do not provide visibility or security while users interact with sensitive resources. Because iboss ZTNA is part of the iboss Zero Trust SSE, all connections automatically have protection applied, including CASB, malware defense, DLP, Exact Data Match, compliance policies, HTTPS decrypt and logging at scale and delivered in the cloud.

PAIN POINT

VPNs provide too much access to onsite resources – VPNs cannot provide granular access controls and allow users to access any resource in the office when connected, which increases risk

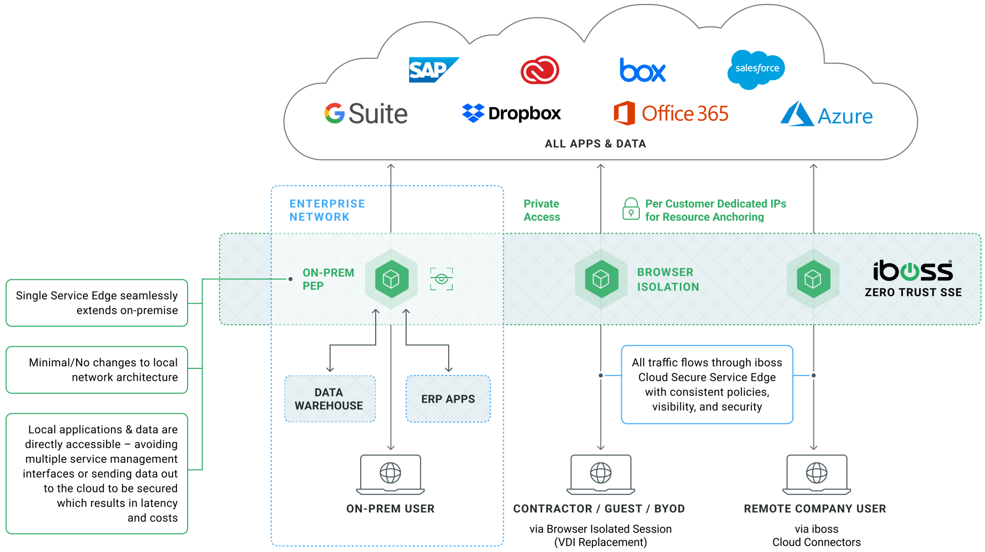
iboss SOLUTION

ZTNA provides granular access controls – The iboss Zero Trust SSE provides per-app access controls and automatically denies all other resources. It also provides a complete security stack and logging to reduce risk and increase compliance.

Learn more
www.iboss.com

iboss’ Zero Trust Security Service Edge

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


SAP
box
salesforce
G Suite
Dropbox
Office 365
Azure
ALL APPS & DATA
ENTERPRISE NETWORK
Private Access
Per Customer Dedicated IPs for Resource Anchoring
ON-PREM PEP
BROWSER ISOLATION
iboss ZERO TRUST SSE
Single Service Edge seamlessly extends on-premise
Minimal/No changes to local network architecture
Local applications & data are directly accessible – avoiding multiple service management interfaces or sending data out to the cloud to be secured which results in latency and costs
DATA WAREHOUSE
ERP APPS
All traffic flows through iboss Cloud Secure Service Edge with consistent policies, visibility, and security
ON-PREM USER
CONTRACTOR / GUEST / BYOD
via Browser Isolated Session (VDI Replacement)
REMOTE COMPANY USER
via iboss Cloud Connectors

The iboss Zero Trust SSE consolidates VPNs, Proxies, and VDI into a single solution to reduce complexity and increase security while reducing costs. ZTNA capabilities within the iboss Zero Trust SSE support SSO authentication, including MFA, and will perform SAML SSO before access to a resource is allowed. This allows SSO to be extended to legacy applications and services that do not support it by allowing iboss to perform SSO before access is granted. In addition, CASB, malware defense, compliance policies, DLP, and logging are applied to every connection to increase security, compliance, and visibility.

The iboss Zero Trust SSE provides extensive network and security capabilities that completely replace VPN, Proxies, and VDI with ZTNA, Security 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 but must install a VPN to obtain it.

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, all without software or a VPN.

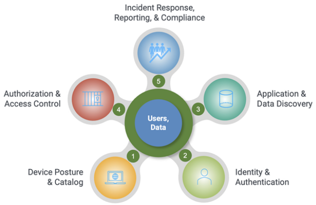
Learn more
www.iboss.com

A Complete Platform: iboss Zero Trust Security Service Edge

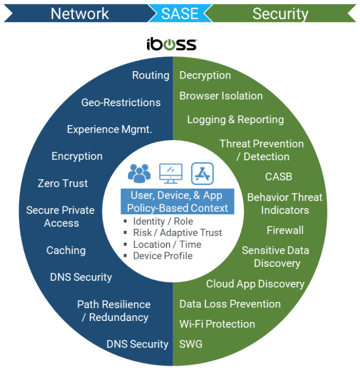
Providing both Connectivity and Advanced SaaS Security Services

iboss SASE Benefits & Use Cases

- Significantly improves connectivity performance for all users, including remote workers
- Reduces complexity, cost & operational overhead related to managing network security infrastructure
- Enhances security with inspection of all content including files, data, and cloud application traffic
- Zero Trust enables connectivity directly and securely to all apps based on role
- Transparency for users / easy to use & deploy
- Increased effectiveness of network & security staff
- Reduces proxy and security appliance bloat
- Allows centralized security policies to protect all transactions and sensitive cloud data
- Eliminates costly proxy appliance mgmt. overhead


Incident Response, Reporting, & Compliance
5
Authorization & Access Control
4
Application & Data Discovery
3
Users, Data
Device Posture & Catalog
1
Identity & Authentication
2

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 Security 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, Security 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 VPN to improve security by providing access on a per-application basis

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

Achieve higher security with continuous adaptive access that evaluates every request for security and compliance

Force MFA and SSO for all applications and services, including legacy applications that do not support SAML

Gain visibility from detailed logging for every interaction between users and sensitive private resources

Ensure devices are compliant before accessing sensitive resources, such as ensuring the device firewall is on, antimalware is running, and the disk is encrypted

Learn more
www.iboss.com