SOLUTION BRIEF

iboss

Replace VDI with Browser Isolation

The iboss Zero Trust SSE replaces VDI with Browser Isolation to improve security and reduce costs

CHALLENGES

Legacy VDI is typically used to protect sensitive resources in high-risk situations where data loss is more likely to occur. For example, with VDI, Call Center agents interacting with customer data can do so through a VDI pane-of-glass preventing data from touching agent devices. This is important for security and compliance regulations such as GDPR, which require data to remain within geographical regions. If Call Center agents are not located within GDPR regions, VDI can allow them to interact with the customer data while keeping the data compliant and remote. VDI is also used for contractor and third-party access to sensitive resources so that data from those applications do not leave the organization and land on untrusted devices. However, VDI is expensive to deploy and manage and requires a lot of infrastructure and subscription costs. To make things worse, hosting the infrastructure necessary to run VDI is even more expensive in high-cost regions, such as India or Asia, where major Call Centers are operated. In addition, VDI does not provide security and visibility as users interact with resources, as connections within the VDI session do not run through a deep-content inspection proxy. This increases risk due to uncontrolled and unmonitored access.

KEY BENEFITS:

Quickly replace VDI with Browser Isolation to greatly reduce infrastructure costs related to VDI

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

Provide isolated VDI-like Browser Isolated sessions to Call Center agents instantly, in any region, to reduce risks and improve security

Provide contractor and third-party access to specific resources through Browser Isolation to prevent sensitive data from leaking to untrusted guest devices

Copyright © 2023 iboss. All Rights Reserved.

SOLUTION

The iboss Zero Trust Security Service Edge is an advanced security solution that completely replaces the functionality delivered by legacy VDI with a global consolidated cloud security service that includes Browser Isolation. Browser Isolation is the modern replacement for VDI and requires no infrastructure deployments. Browser Isolation uses the end-user's browser to form a VDI-like interface to authorized applications. And because the iboss Zero Trust SSE includes ZTNA, CASB, malware defense, compliance policies, and logging, all interactions inside the isolated browser session have security applied and log events generated for visibility. Browser Isolation supports SSO with MFA so that users can be authenticated before gaining access to sensitive resources. Data from those resources never touches end-user devices ensuring data remains safe. The iboss Zero Trust SSE includes Browser Isolation that is available everywhere, instantly, which results in fast time-to-value as the need to purchase, deploy and manage infrastructure is eliminated. The costs associated with VDI infrastructure are also eliminated, substantially reducing costs.

KEY BENEFITS:

- Quickly replace VDI with Browser Isolation to greatly reduce infrastructure costs related to VDI
- Consolidate point products such as VPN, Proxies, and VDI with ZTNA, SSE, and Browser Isolation for lower costs
- Provide isolated VDI-like Browser Isolated sessions to Call Center agents instantly, in any region, to reduce risks and improve security
- Provide contractor and third-party access to specific resources through Browser Isolation to prevent sensitive data from leaking to untrusted guest devices
- Gain visibility from detailed logging for every interaction between users and sensitive private resources within the isolated browser session for better security
- Eliminate the need for third parties to install VPN software to gain access to private resources by leveraging Browser Isolation instead

SOLUTION CAPABILITIES

Provide VDI-like access to any resource through Browser Isolation to prevent data loss

Connect Call Center agents to sensitive resources through a pane-of-glass to ensure data remains in-region compliant and reduce the risk of data loss

Connect contractors and third parties with SSO to private resources, with data separation, without the need to install VPN software

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

Learn more
www.iboss.com

Copyright © 2023 iboss. All Rights Reserved.

KEY SOLUTION CAPABILITIES:

- Provide VDI-like access to any resource through Browser Isolation to prevent data loss
- Connect Call Center agents to sensitive resources through a pane-of-glass to ensure data remains in-region compliant and reduce the risk of data loss
- Connect contractors and third parties with SSO to private resources, with data separation, without the need to install VPN software
- 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

PAIN POINTS

Pain Point	iboss Solution
VDI Infrastructure is Expensive – VDI requires expensive infrastructure and data center space to operate	Replace VDI with Browser Isolation – Browser Isolation eliminates the need for infrastructure and data center space reducing both CAPEX and OPEX substantially
Call Center agents interact with high-risk customer data – Call Center agents need to support customers by accessing sensitive data, but the risk of data loss, breach, or compliance violations is high	Browser Isolation Provides Isolated Access – Browser Isolation completely separates the data and application from Call Center agents through a pane of glass preventing data from leaking to unauthorized locations.
Contractors Need to Install VPN for Access – Contractors need to install VPNs to gain needed access to sensitive resources, but the risk is high for data loss	Browser Isolation Provides Agentless SSO Access – Browser Isolation can authenticate and provide access for contractors with no software installs while ensuring data remains within the organization by protecting it with a pane-of-glass
VDI Provides little Access Security + Visibility -When users access resources through a VDI session, no security is applied to those interactions, and no log events are generated due to a lack of proxy capability	Browser Isolation + SSE - The iboss Zero Trust SSE runs all Browser Isolated sessions through the Security Service Edge, which applies security and generates log events for all interactions within the isolated session.

PAIN POINT

VDI Infrastructure is Expensive – VDI requires expensive infrastructure and data center space to operate

iboss SOLUTION

Replace VDI with Browser Isolation – Browser Isolation eliminates the need for infrastructure and data center space reducing both CAPEX and OPEX substantially

Learn more
www.iboss.com

Copyright © 2023 iboss. All Rights Reserved.

USE CASES / BUSINESS VALUE:

Use Case/Challenges	Solution Description	Benefits
Need to provide sensitive customer data access to Call Center agents	The iboss Zero Trust SSE provides Browser Isolation which separates customer data from Call Center agents to reduce the risk of data loss.	Quickly grant Call Center agents access to apps and data they need to support customers without increasing the risk of breach or data loss.
Need to eliminate VDI infrastructure to reduce costs	The iboss Zero Trust SSE includes Browser Isolation which does not require any infrastructure and is delivered directly from the cloud as a service.	Substantially lower costs from VDI infrastructure and the data center space required to operate it.
Need to eliminate or reduce the data center footprint.	Because the iboss Zero Trust SSE Browser Isolation runs within the iboss service, it requires no data center space. Infrastructure related to VDI can be eliminated by reducing or eliminating the data center footprint.	Substantially lower operating and infrastructure costs as well as reduced management overhead.
Need to gain logging visibility and apply security to all interactions within a VDI session	The iboss Zero Trust SSE Browser Isolation capability runs through the iboss Security Service Edge and automatically benefits from CASB, malware defense, compliance controls, CASB, and logging.	Reduce security risk and increase compliance with increased security and visibility.
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

Call Center agents interact with high-risk customer data – Call Center agents need to support customers by accessing sensitive data, but the risk of data loss, breach, or compliance violations is high

iboss SOLUTION

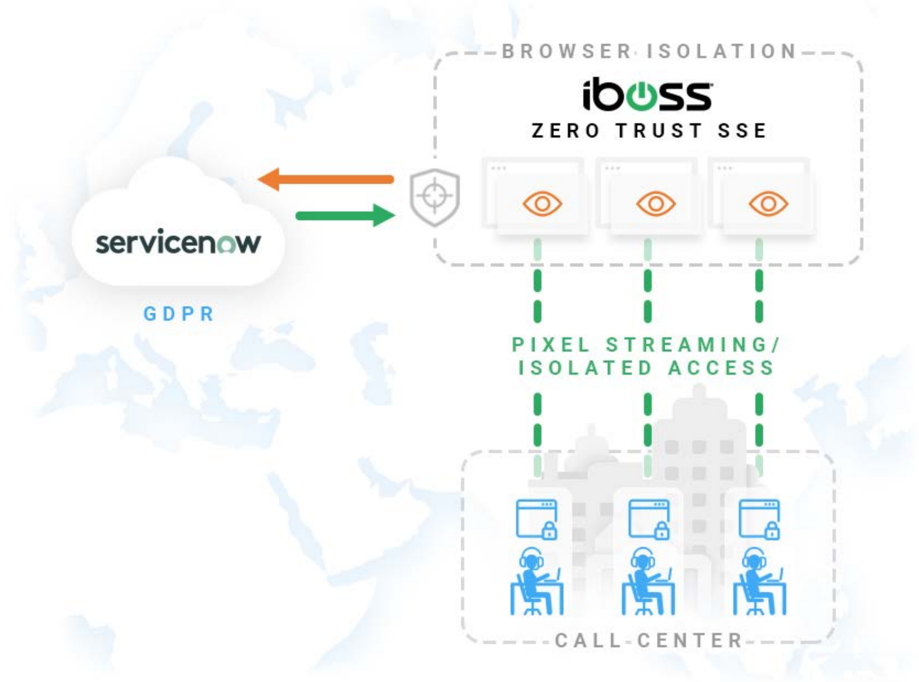
Browser Isolation Provides Isolated Access – Browser Isolation completely separates the data and application from Call Center agents through a pane of glass preventing data from leaking to unauthorized locations.

Learn more
www.iboss.com

Copyright © 2023 iboss. All Rights Reserved.

TECHNICAL SOLUTION:

VDI has been the solution used to connect users to high-risk applications when the risk of data leakage is high because it can provide access through a pane-of-glass that separates the application and data from the user. Although it is a powerful mechanism to reduce risk, it requires substantial investment in infrastructure and data center space. VDI also does not natively support deep-content security or logging because it is a point product that lacks a proxy.



The iboss Zero Trust SSE can solve the issues related to VDI by delivering the same capability through Browser Isolation. Browser Isolation separates users from sensitive resources with a pane-of-glass, just like VDI, except it uses the end user's browser to provide isolated access. This prevents the application and data from touching high-risk users and devices to reduce the risk of breaches and data loss.

In addition, VDI does not provide visibility or security while users interact with sensitive resources. Because iboss Browser Isolation 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

Contractors Need to Install VPN for Access – Contractors need to install VPNs to gain needed access to sensitive resources, but the risk is high for data loss

iboss SOLUTION

Browser Isolation Provides Agentless SSO Access – Browser Isolation can authenticate and provide access for contractors with no software installs while ensuring data remains within the organization by protecting it with a pane-of-glass

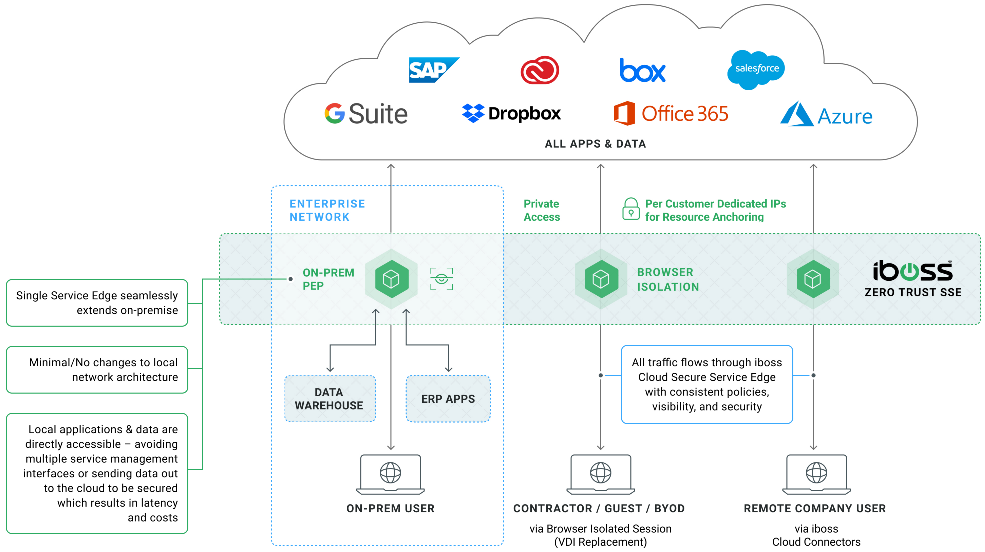
Learn more
www.iboss.com

Copyright © 2023 iboss. All Rights Reserved.

REPLACE VDI WITH BROWSER ISOLATION

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
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
ON-PREM PEP
BROWSER ISOLATION
iboss ZERO TRUST SSE
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

VDI Provides little Access Security + Visibility -When users access resources through a VDI session, no security is applied to those interactions, and no log events are generated due to a lack of proxy capability

iboss SOLUTION

Browser Isolation + SSE - The iboss Zero Trust SSE runs all Browser Isolated sessions through the Security Service Edge, which applies security and generates log events for all interactions within the isolated session.

Learn more
www.iboss.com

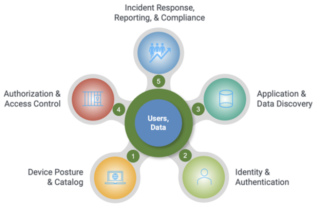
Copyright © 2023 iboss. All Rights Reserved.

A Complete Platform: ZTNA + Security Service Edge

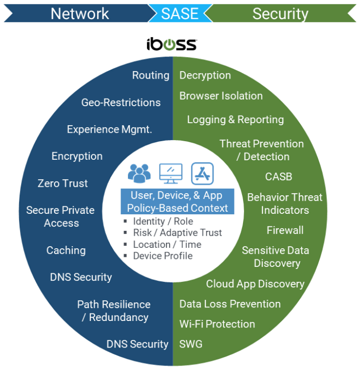
Providing both Connectivity and Advanced SaaS Security Services

iboss SASE Benefits & Use Cases

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


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

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**.

Copyright © 2023 iboss. All Rights Reserved.

KEY BENEFITS:

Quickly replace VDI with Browser Isolation to greatly reduce infrastructure costs related to VDI

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

Provide isolated VDI-like Browser Isolated sessions to Call Center agents instantly, in any region, to reduce risks and improve security

Provide contractor and third-party access to specific resources through Browser Isolation to prevent sensitive data from leaking to untrusted guest devices

Gain visibility from detailed logging for every interaction between users and sensitive private resources within the isolated browser session for better security

Eliminate the need for third parties to install VPN software to gain access to private resources by leveraging Browser Isolation instead

Learn more
www.iboss.com