Replace VDI with Browser Isolation + Security Service Edge

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

SOLUTION BRIEF

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

SOLUTION BRIEF

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

KEY BENEFITS: