iboss Zero Trust Security Service Edge Certified Secure Test Report

27 March 2023

DR230227G

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Miercom was engaged by iboss to independently assess its Zero Trust Security Service Edge solution against the latest threats by examining protective features, refined controls, and user experience.

When choosing a security solution, the iboss Zero Trust Security Service Edge platform is a viable answer to typical and atypical network threats. Traditional security products protect against malicious actors crossing the network perimeter, blocking anything that puts access into the wrong hands. But now, with more users accessing their networks remotely, this border might as well have dissolved – leaving networks at serious risk.

Office networks need a way to protect users, on-site and remote when this perimeter extends to the cloud. Threat intelligence should be applicable from any location, at any time, and from a wide variety of engines, to provide a robust and granular way to deliver network security.

The iboss Zero Trust Security Service Edge offers the flexible, scalable, and reliable security that enterprises should have when the perimeter is not obvious. Using its cloud security service that includes malware engines and a large number of threat and reputation feeds, the iboss platform provides comprehensive malware, compliance, and DLP protection. No appliances are needed; this cloud-based solution provides Software as a Service (SaaS) controls for cloud security and compliance regulation of today's multi-cloud environment. This platform is fully integrable with third-party clouds, such as Microsoft Azure, by leveraging its unique architecture, which uses containerized cloud gateways to extend its capabilities from iboss's global cloud backbone to other cloud edges to provide fast and thorough protection for a high-quality user experience.

Unlike other security solutions, the iboss Zero Trust Security Service Edge can scan in-transit data within the cloud before reaching the user or device. Its rich feature set successfully prevents complex malware, infections, and data loss to save time and cost for IT personnel and data breach management. This subscription-based service requires no hardware upgrades or additional licensing to let networks reap the latest and greatest benefits with less overhead. Most importantly, the Zero Trust platform automatically scales to serve any user's bandwidth and capacity demands, from any location. Highlights from testing are as follows:

Key Findings of the iboss Zero Trust Security Service Edge:

- 100% protection against advanced evasive techniques, AETs, advanced persistent threats, backdoor malware, remote access trojans (RATs), and particularly ransomware – a costly malware affecting networks today
- The same pattern can be seen in iboss's accuracy rates at Z+3 and Z+7 days after initial detection, which is both higher than the average accuracy rate for detecting malware at Z+3 and Z+7 days across all systems

- iboss Zero Trust Security Service Edge detects malware with a 90% accuracy rate within one day of detection, which is higher than the average accuracy rate of 64% across all systems
- 99% average malware security efficacy, 26% higher than the industry average tested with Miercom to date
- 98% security efficacy against complex, active malware
- Consolidates functionality of VPN, Proxies and VDI into single service stack to improve security, performance, and end user experience
- Traditional, high-cost technologies are consolidated and replaced by higher performance, cloud-based solutions: Zero Trust Network Access (ZTNA) to replace VPN, Brower Isolation to eliminate VDI, and SSE to protect local and remote users in place of legacy proxies
- The iboss Zero Trust SSE provides local protection with on-site gateways that allow for faster, smoother migration capabilities that can reduce high-cost renewals and associated labor costs seen in traditional on-premise topologies

Based on our findings, the iboss Zero Trust Security Service Edge platform was validated for its protection against malware, malicious URLs and data loss by testing within a simulated office network deployment. Its extension of security across a distributed workforce was easily implemented with a single configuration, offering protection that earned it the **Miercom Certified Secure** certification.

Robert Smithers

CEO, Miercom

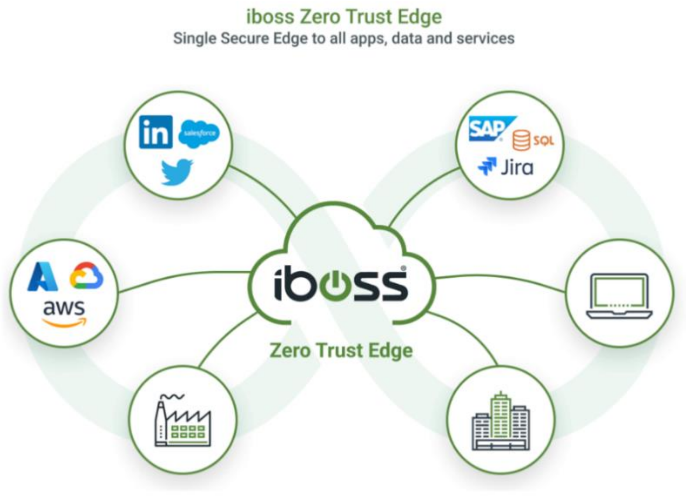
2.0 Introduction

2.1 Products Tested

iboss Zero Trust Security Service Edge

CLOUD IS THE FUTURE

Cloud technology is the lifeblood of modern technological progress and a trendsetter for the next generation in the modern tech industry. During the early stages of the COVID-19 pandemic, businesses around the world began implementing the work-from-home model and various digital technologies into their operations.



All users, data, and services are connected through iboss global cloud security service

Another unintended consequence of this new remote working norm was the proliferation of cloud models. And, as organizations began to adopt cloud models at a faster rate, the models themselves began to evolve at a faster rate as well. As a result, cloud technology has grown significantly in recent years. The iboss Zero Trust Security Service Edge platform provides elastic security for distributed workforces without needing network security appliances. No matter how much bandwidth or cloud capacity is used, appliances are not required – iboss has 100+ points of presence around the world to provide coverage and security capabilities for any location.

USER-BASED SECURITY

iboss protects user cloud access regardless of device or location. Because it works natively with cloud-based applications, there is no "network perimeter" with iboss. The remote user notices no difference between on-site and off-site cloud application use, and protection adapts to their network location as if they were always in the office. iboss's distinct approach is to provide granular user-based security rather than the perimeter-based protection provided by public cloud gateway security solutions.

Cloud security solutions that lack modern containerization for their cloud gateways introduce security risks (for example, SSL decryption private keys), have uncontrolled automatic update cycles, prevent extending IP address identification for easy third-party integration, and lack geographic control.

MALWARE ANALYSIS

The iboss Zero Trust Security Service Edge platform is unlike traditional gateways with its unique, cloud-based malware analysis. Its unconventional design reveals a wide range of threats and allows for inspection and control of the network from local, remote, or mobile endpoints.

iboss protection makes use of these modules:

- Cloud Security
- CASB
- Malware Defense
- Data Loss Prevention
- Compliance Policies
- Logging
- ZTNA
- Browser Isolation
- Continuous Adaptive Access
- Enable a Hybrid Work Environment
- Ease of Use and Deployment

A user can connect into the platform from any device – on-site or mobile – to receive protection from anywhere in the world. Malware data feeds use a consolidated library of signatures from hundreds of alliance engine sources – all from the cloud with no need for physical hardware. The cloud-based SaaS platform redirects traffic to overcome architectural challenges without the need for Software Defined WAN (SD-WAN) or perimeter extension solutions.

Users are shielded against malicious activity via malicious websites, harmful malware files, and the extraction of personally data in real-time and from any geographical location.

2.2 Test Focus

Protective Features

- Malware Detection Engine
- Phishing URL Blocking
- Zero Trust Analysis

3.0 How We Did It

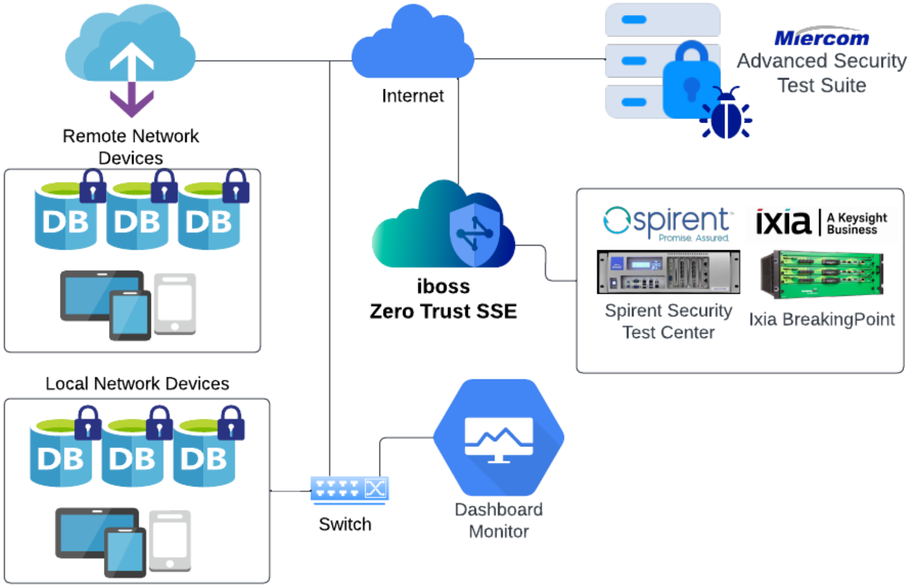
To test the functionality of the System Under Test (SUT), a custom-built network was created to simulate a real-world deployment. Traffic was generated and delivered through the network, along with malicious samples, to evaluate the ability of the SUT to detect, prevent and respond to threats.

All results regarding security efficacy, monitoring, intelligence and reporting visibility were observed and recorded. These areas were analyzed to determine useful techniques and experiences of the security platform.

3.1 Test Environment

We conducted tests with all security services enabled and challenged the iboss Zero Trust SSE platform's ability to block the latest malware and phishing URL samples. These modern web-based attacks increase the threat level against organizations globally. The majority of which exploit weaknesses at the network perimeter. Cloud security offers the best protection against this generation of cyberattacks by analyzing beyond the perimeter for more robust security.

Out testing specifically focused on the ability to prevent new malware variants within the following time frames: 1 day, 3 days, and 7 days of their discovery. We also analyzed the prevention of new phishing sites within 1 day and 14 days of discovery.



Source: Miercom 2023

Testing employed remote and local network devices connected to the Internet and the local network via a switch. To implement malware and phishing attacks, we used our proprietary security test suite, along with the latest exploits from Spirent and Keysight Ixia test tools. Traffic was simulated using the Keysight Ixia BreakingPoint to recreate a realistic network environment.

Malware Samples

In this report, Zero+1 Day Malware (one day past Zero-Day discovery) means newly discovered malware on the first day of discovery. These malware samples are less likely to be known by any vendors' signature detection mechanisms in the first 24 hours. Zero+3 Day Malware is used for malware samples uploaded at least 'three days ago' to common virus registries like VirusTotal and therefore should have been detected by most leading security vendors. Zero+7 Malware consists of threat uploaded at least 'seven days ago' to common virus registries.

4.0 Malware Efficacy

4.1 Malware Detection Engine

The malware detection capabilities of the SUT were assessed in this section of the testing.

Testing focused on the protection against the following threat categories listed below. The Miercom malware server simulates a hacker's attack server which hosts thousands of malware samples that characterize the breadth of coverage provided by the iboss *Advanced Malware Defense* engines.

Samples from the Miercom malware server are used in industry-wide studies of malware detection for network security devices. Common malware types are botnets and Remote Access Trojans (RATs). An emphasis is placed on active threats, advanced evasion techniques and advanced persistent threats which are more complex and challenging categories for security solutions to identify. Detection results reveal individual approaches to malware detection, as well as its granularity.

The SUT was an intermediary between untrusted and trusted zones of the simulated network. A simulated attack from the untrusted zone consisted of an attempted download of a malicious file. A successful block was logged when the simulated victim client cannot download the malware sample.

Miercom Malware Samples

Miercom Malware Set
Active Threat Dynamic malware (e.g. worm) that continues damaging systems until controlled and contained
Backdoor Remote access attacks that use port binding, control and command servers, and dormant malware to infiltrate networks using legitimate programs or platform to go unrecognized
Botnets Communicating programs delivering spam and Distributed Denial of Service (DDoS) attacks
Legacy Relatively old, and typically known, malware expected to be detected; however, sometimes systems disregard such antiquated threats – allowing them to still attack networks
Malicious Documents Seemingly benign electronic documents (e.g. MS Word, Adobe PDF) that contain malicious coding ("macros") alongside plain-text data to seem legitimate while infecting upon opening
Remote Access Trojans (RATs) Trojans disguised as legitimate software which remotely control victim once activated
The Onion Router (TOR) Malware with multi-layer encryption that collects personal data and sends to C&C server

Advanced Threats

Advanced Evasion Techniques (AETs)

Combined evasion tactics that create multi-layer access

Advanced Persistent Threats (APTs)

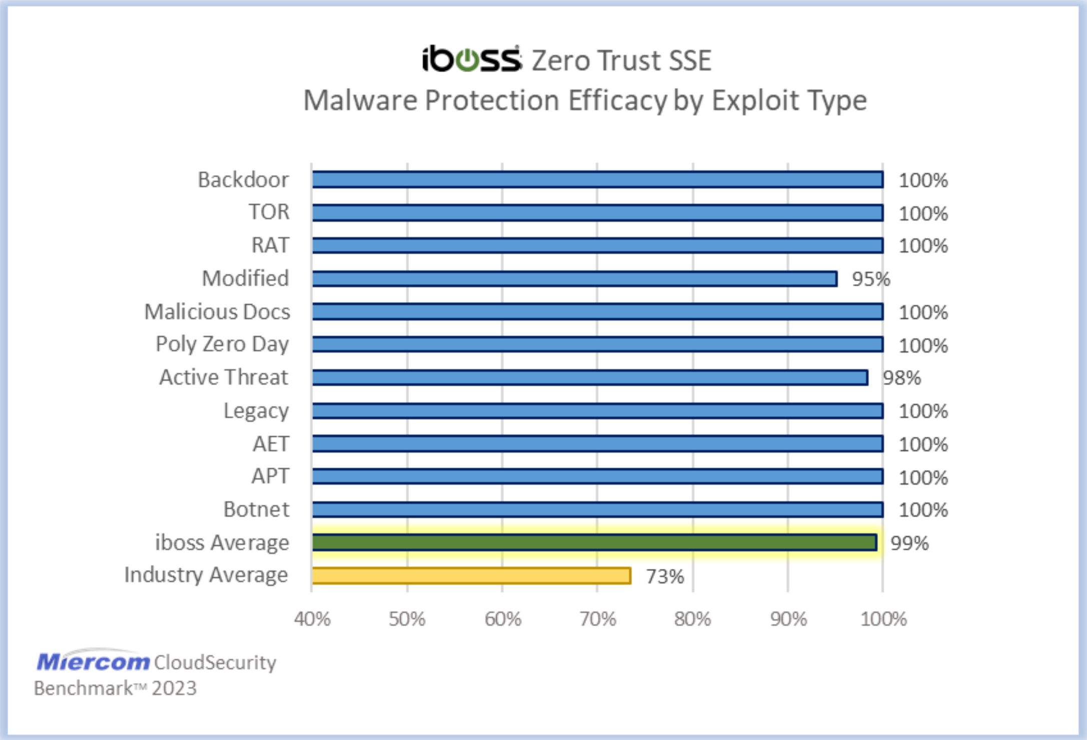
Continuous hacking with payloads opened at the administrative level

Modified Malware

Original malware, detectable by public repositories, is modified with techniques that allow it to now evade detection

Polymorphic, Zero-Day Malware

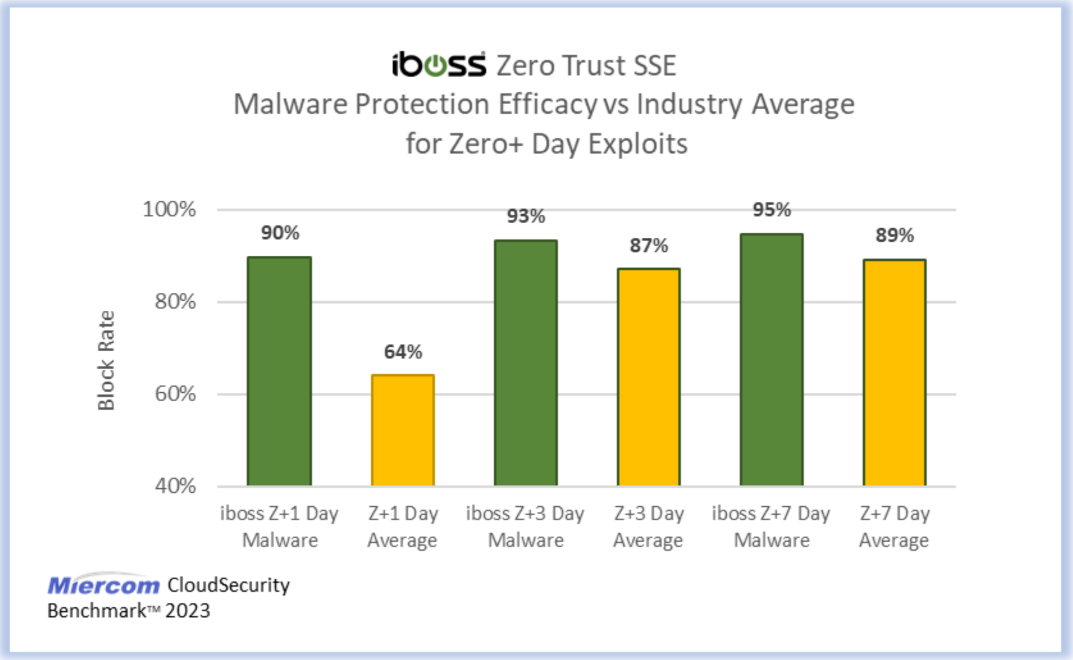
Constantly changing, difficult to detect; exploit known vulnerabilities



iboss Zero Trust Security Service Edge prevented 100% of Backdoor, TOR, RAT, Malicious Docs, Polymorphic Zero Day, Legacy, AET, APT, and Botnet malware samples. It had nearly perfect protection against both active and modified threats. The average iboss malware protection was 99% - 26% higher than the average industry malware prevention product or service.

4.2 Malware Average Z+1 Day, Z+3 Day and Z+7 Day

Miercom tested the iboss Zero Trust Security Service Edge versus the industry average. We found that iboss outperformed the industry average on blocking all Zero+1 (Z+1) Day, Zero+3 (Z+3) Day and Zero+7 (Z+7) Day Malware tested.

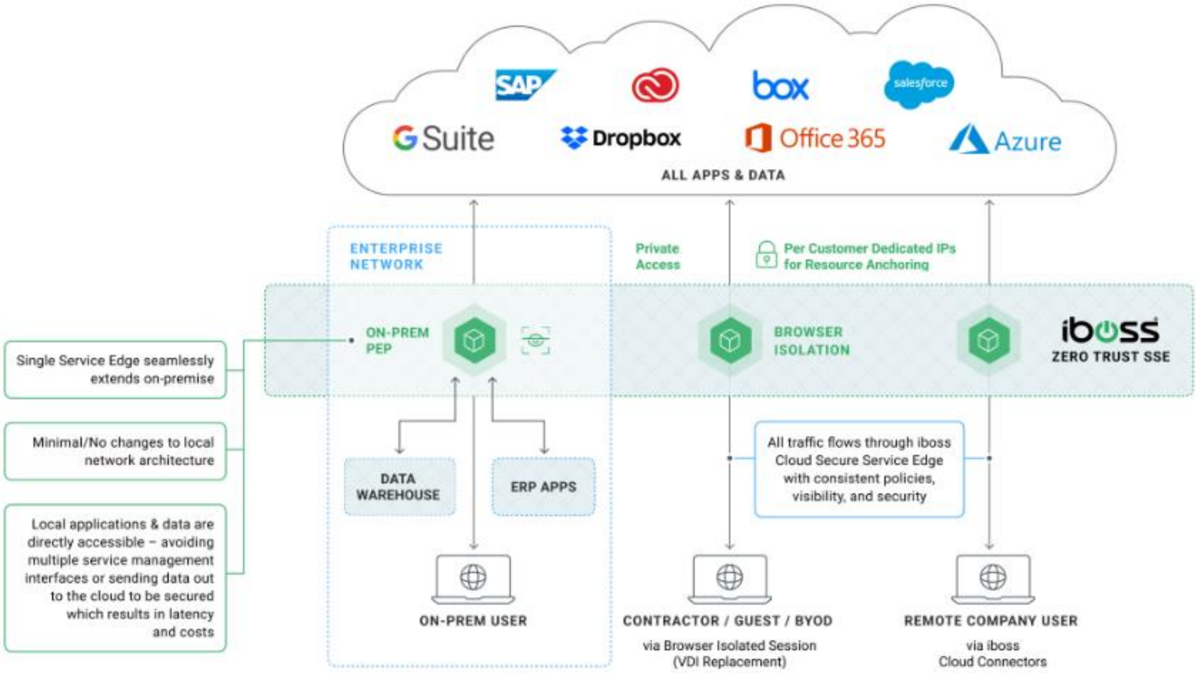


iboss Zero Trust Security Service Edge prevents malware with a 90% accuracy rate within one day of detection, which is higher than the average rate of 64%, across all systems. This means that iboss prevents more malware in a single day than the average system. The same pattern can be seen in iboss' efficacy rates at Z+3 and Z+7 days after initial detection, which are both higher than the average efficacy rate for blocking malware at Z+3 and Z+7 days across all systems, at 93% and 95% efficacy.

5.0 Zero Trust Analysis

iboss is the only cloud security vendor that meets every Tenet and network requirement set by the NIST 800-207 Zero Trust Architecture to protect your users anywhere.

The iboss Zero Trust Security Service Edge (SSE) consolidates functionality of VPN, Proxies and Virtual Desktop Infrastructure (VDI) into a single service stack to improve security, performance, and end user experience.

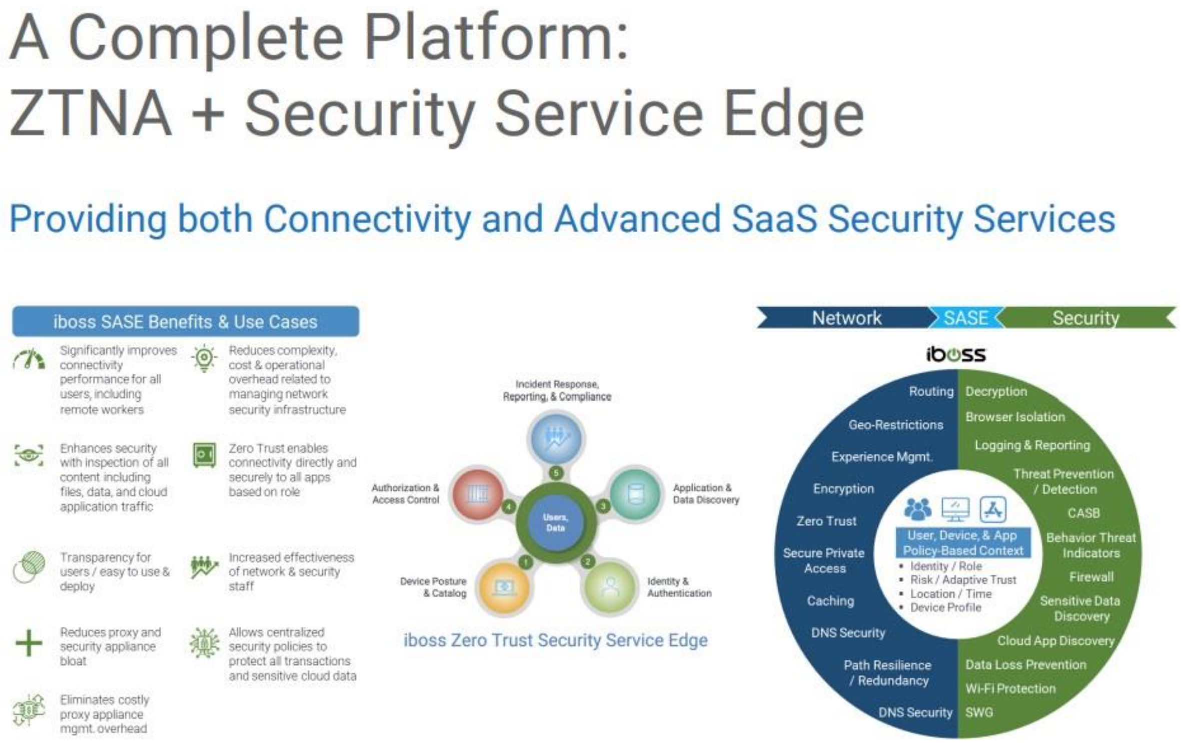

SAP
box
salesforce
G Suite
Dropbox
Office 365
Azure
ALL APPS & DATA
ENTERPRISE NETWORK
Private Access
Per Customer Dedicated IPs for Resource Anchoring
ON-PREM PEP
BROWSER ISOLATION
iboss
ZERO TRUST SSE
Single Service Edge seamlessly extends on-premise
Minimal/No changes to local network architecture
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

Source: iboss 2023

iboss Zero Trust Security Service Edge (SSE) consolidates technology for a better user experience and substantially lower costs. It includes: Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), malware defense, compliance policies, Data Loss Prevention (DLP), Browser Isolation, and logging for every resource request. It also replaces legacy proxies via cloud security to protect all workers, local or remote. Its optional on-site gateways that can be deployed to the data center offer local protection, and fast migration capabilities, to secure the network while reducing the high-cost renewals seen with traditional on-premise topologies. Other functionality includes:

- ZTNA replaces VPN, providing background security to users connected to private applications and data
- Browser Isolation removes the need for Virtual Desktop Infrastructure (VDI), isolating application and data access via the cloud to eliminate the need for infrastructure or data center space
- Automatically prevents infected devices from damaging resources, without requiring manual intervention, by cutting resource access as soon as a device becomes infected
- Reduces risks through analysis of applications, data, and services to uncover shadow IT, unsanctioned applications and risky cloud services

The iboss Zero Trust SSE inspects all content for malware, DLP, CASB, Compliance, Policies, and Logging. In addition to the iboss threat intelligence, the iboss platform leverages threat intel from other sources such as Verizon threat intel and applies that to every transaction.



A Complete Platform:
ZTNA + Security Service Edge

Providing both Connectivity and Advanced SaaS Security Services

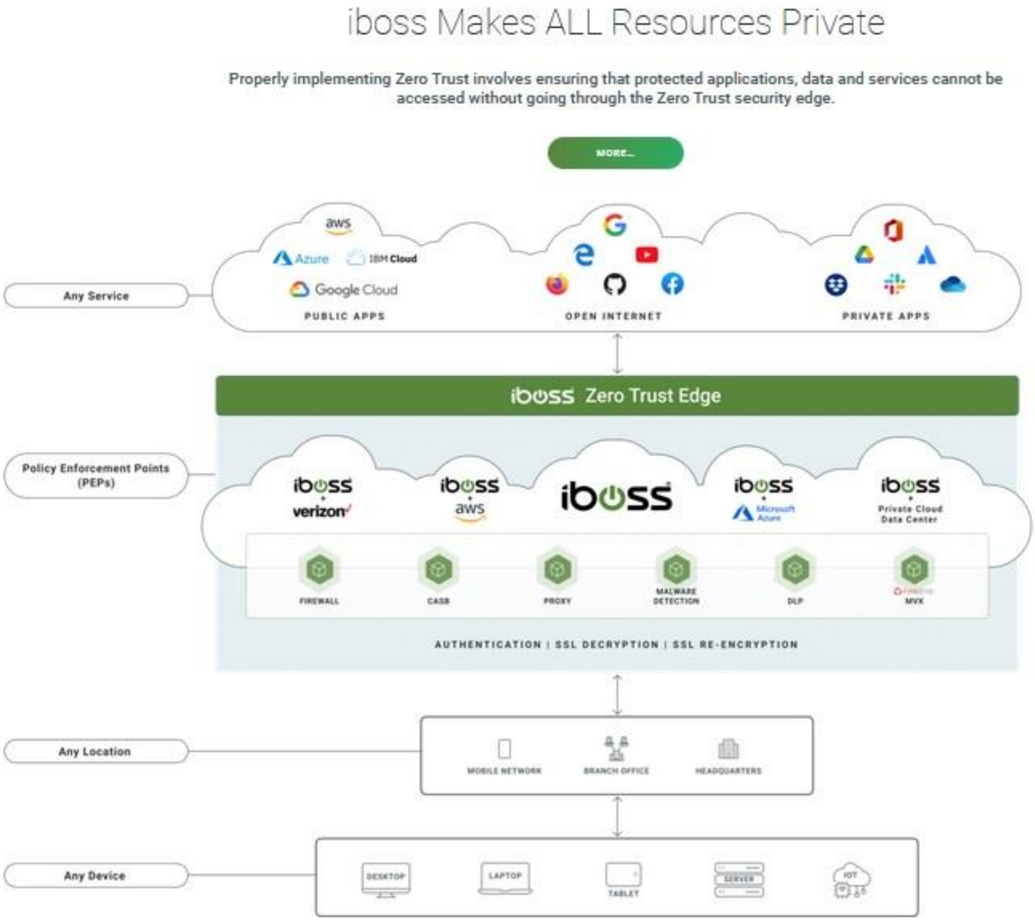
iboss SASE Benefits & Use Cases

- 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
Application & Data Discovery
3
Identity & Authentication
2
Device Posture & Catalog
1
Authorization & Access Control
4
Users, Data

iboss Zero Trust Security Service Edge

The iboss Zero Trust Security Service Edge includes CASB, malware defense, DLP, browser isolation and logging. It also includes the Verizon threat intel that extends iboss threat intel to over 150 threat feeds for the outstanding protection.



iboss Makes ALL Resources Private

Properly implementing Zero Trust involves ensuring that protected applications, data and services cannot be accessed without going through the Zero Trust security edge.

iboss runs the largest containerized cloud security service which provides the capabilities of the Zero Trust Security Service Edge. This cloud security service processes over a 150 billion transaction per day on an iboss native backbone for all resources access types. Unlike other vendors, such as Zscaler, who run ZPA in AWS, all transactions run through iboss native POPs.

About Miercom

Miercom has published hundreds of network product analyzes in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyzes, as well as individual product evaluations. Miercom features comprehensive certification and test programs, including Certified Interoperable™, Certified Reliable™, Certified Secure™, and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment of product usability and performance.

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

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document may contain certain vendors' representations that Miercom reasonably verified but is beyond our control to verify with 100 percent certainty.

This document is provided "as is", by Miercom and gives no warranty, representation, or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness, or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your trademarks in connection with any activities, products, or services that are not ours or in a manner that may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects, or developments.

By downloading, circulating, or using this report in any way, you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit miercom.com/tou.