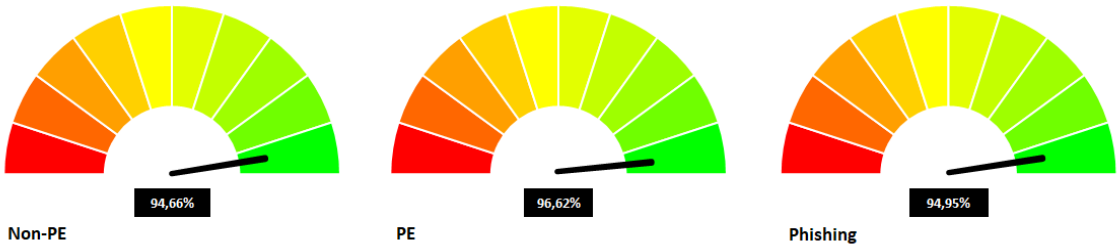
Evaluation of iboss Zero Trust Security Service Edge

A test commissioned by iboss and performed by AV-TEST

Date of the test report: June 15, 2023 (version 1.00)

Executive Summary

In March 2023, AV-TEST performed a test of the “iboss Zero Trust Security Service Edge” focusing on blocking malicious URLs and phishing websites as well as false positive avoidance. The test evaluates the protection at 'time zero' as well as on differences in the detection found 48 hours later.



To ensure a fair review, iboss did not supply any samples (such as malicious or clean samples, URLs or associated metadata) and did not influence or have any prior knowledge of the samples tested or the testing methodology. All links and malicious samples tested were verified by AV-TEST as recent and active.

The test focused on the detection rate of links pointing directly to portable executables (PEs) malware (e.g., EXE files), links pointing to other forms of malicious files (e.g., html, JavaScript) as well as phishing URLs. A total of 3,578 malicious samples were tested in the first run. The samples were weighted towards phishing URLs (36.33%), and PE malware (27.98%) while non-PE malware consisted of the remaining (35.69%) of samples. In the retest, 2,812 malicious samples were tested and were slightly different weighted towards phishing URLs, PE and non-PE malware.

Besides this, we evaluated the false positive rates using downloads for well-known applications from http and https websites. An additional false positive test was performed against known clean popular websites from Alexa’s top list. A total of 3,185 test cases were used.

The full details of the test setup and the testing scenarios can be found in the following sections of this test report.

Test Overview

Every second, AV-TEST discovers three to four new malware variants. This sums up to around 9 million new malware every month, or more than 1.35 billion malware objects in total which are included in AV-TEST’s database.

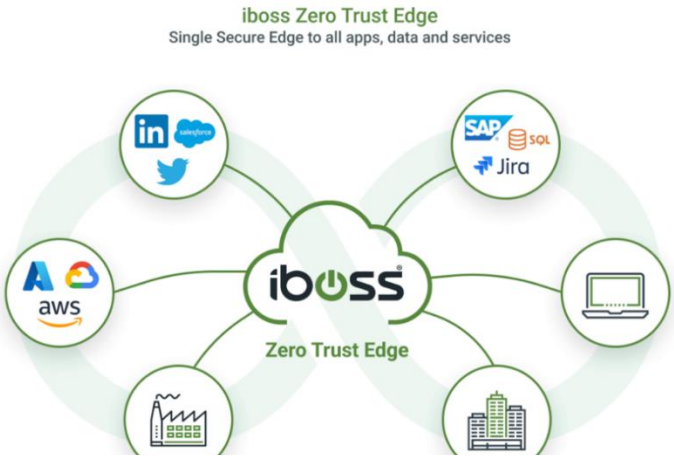
While most malware targets the Windows platform, protection for all operating systems is a required practice. Attaining protection against the growing number of threats is essential for all enterprises. Phishing is a great example of an attack that impacts all operating systems and relies on fooling the end user into thinking the site is legitimate so the attacker can steal sensitive information.

iboss has commissioned AV-TEST to review their iboss Zero Trust Security Service Edge.

Overview of the 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 personal data in real-time and from any geographical location.

Test Cases

All the tests were performed in AV-TEST's laboratory in Magdeburg, Germany. All data used for testing, including all samples URLs and metadata, was exclusively sourced by us.

iboss did not have access to sample URLs before the testing, nor did provide such data for the testing. All samples were previously verified by AV-TEST as known to be malicious. We use static and dynamic analysis of samples to ensure that the domains are actively hosting malicious content at the time of the testing and exhibiting their malicious behavior.

Both performed tests were split into three categories, covering the different types of attacks:

- URLs pointing to malicious PE files (for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually html or php websites, including links to scripts such as JavaScript or VBS)
- Links to phishing websites

A total of 3,578 samples were used for the initial test-run ('time zero'). This included 1,001 malicious links to PE files, 1,277 links to other files with other malicious content (non-PE), and 1,300 samples of phishing websites. For the retest after 48 hours, some URLs didn't work anymore, as they were taken offline (e.g., by the attacker or internet provider). Therefore, only 2,812 test cases were used, including 798 links to PE files, 1,142 links to non-PE files and 872 phishing URLs.

For false positive testing, AV-TEST used the following types of known clean files and websites from http and https sources:

- URLs pointing to clean file downloads (mainly PE for Windows, EXE files)
- URLs with other non-malicious destinations (non-PE files, usually clean html or php websites)

All samples used for the false positive testing were carefully selected and validated. In an exhaustive review by AV-TEST, the samples did not show any signs of malicious behavior and were considered clean. A total of 3,185 clean websites and downloads were used for the initial test (1,266 downloads and 1,919 websites). For the test-run 48 hours later, a total of 3,144 samples could be used (1,220 downloads and 1,914 websites).

All URLs were accessed on virtualized Windows systems running Windows 10 Professional (English, 64 bit), with all patches installed.

All download attempts were triggered using Python scripts to access the URLs for the test. Testing included checking if access to the URL was successful or if it was blocked by the product. The tests were performed during the period of March 9 to April 14, 2023.

Test Results

For PE file URLs, iboss Zero Trust SSE initially scored 95.10% and increased to 96.62% in the retest as its top efficacy test category. Nearly as effective, non-PE file URLs initially scored 92.48% and increased to 94.66% in the retest. Detection of phishing URLs showed also an improvement from the initial score of 92.38% by increasing to 94.95% in the retest. False positives were low in the initial test at 1.51% and stayed at 1.53% in the retest to remain a low risk.

The detailed results of the detection tests are as follows (higher is better):

	Initial 'time zero' test			Retest after 48 hours		
Detection Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of PE malware	1,001	952	95.10%	798	771	96.62%
… of non-PE malware	1,277	1,181	92.48%	1,142	1,081	94.66%
… of phishing URLs	1,300	1,201	92.38%	872	828	94.95%

The retest after 48 hours showed improvements in detection rates for all three areas.

For the false positive testing, the detailed results are the following ones (lower is better):

	Initial 'time zero' test			Retest after 48 hours		
False Positive Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of good applications	1,266	45	3.55%	1,230	45	3.66%
… of popular Alexa URLs	1,919	3	0.16%	1,914	3	0.16%

The slightly increased false positive rate in the second run is mainly caused by the reduced number of samples. However, the risk of a false positive still remains at a low level.

Conclusion

iboss Zero Trust SSE was tested independently by AV-TEST with no knowledge of samples tested or providing samples for the testing. Threat efficacy detection results peaked at 96.62% for PE file URLs in the retest and false positives remained a low risk for initial and retesting.

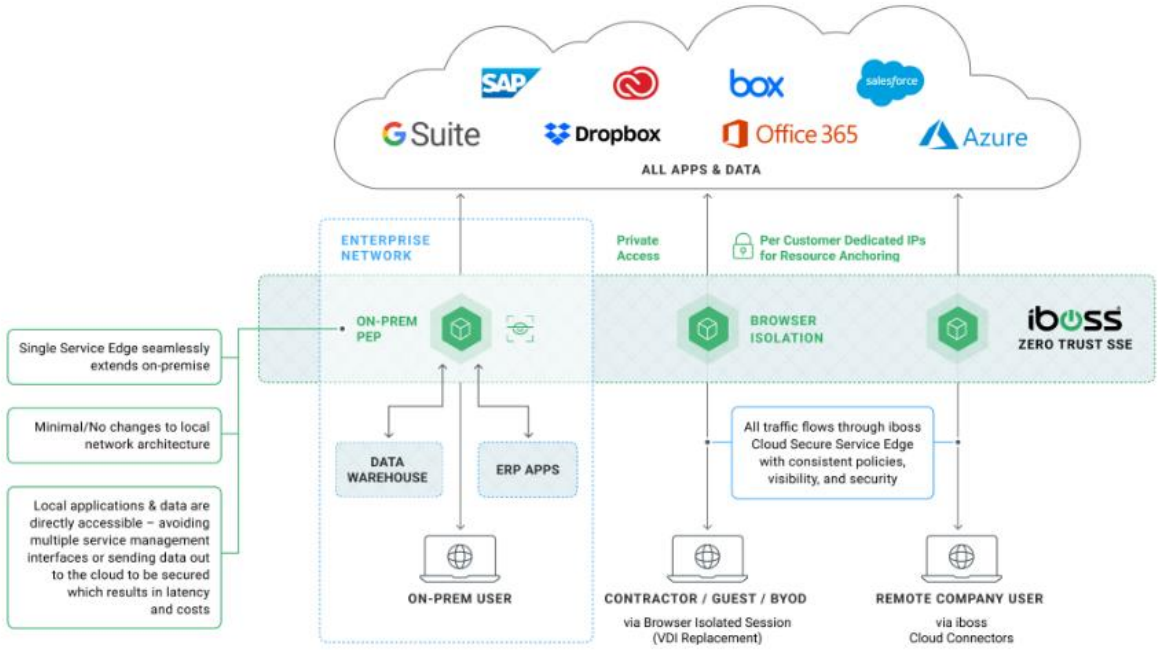
The industry median of the results of all tested SWG products (2022-06 / 2023-06) separated by test categories is for PE 86.52%, Non-PE 90.15% and for phishing URLs 85.44%.

Considering all results of the products tested by AV-TEST iboss is among the top performers of that product category and offers strong protection against the used test cases.

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.



Source: iboss 2023

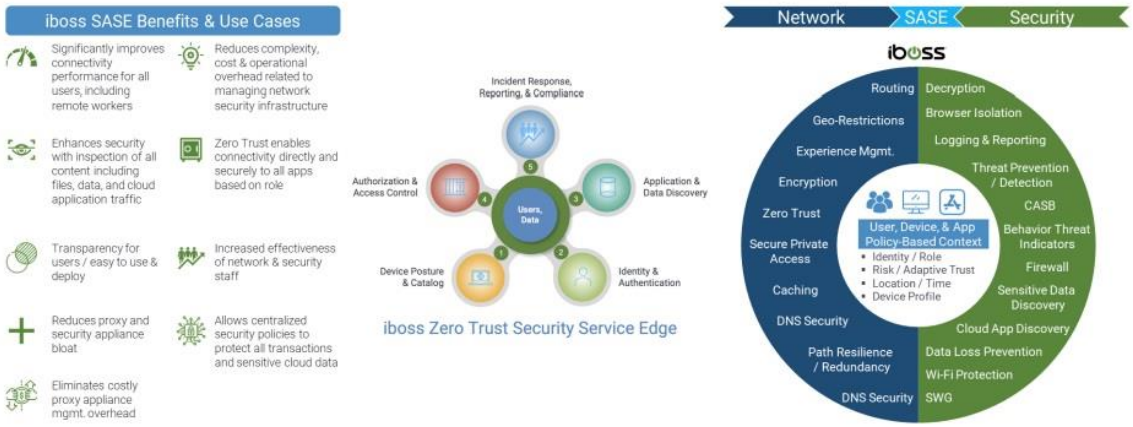
iboss Zero Trust Security Service Edge (SSE) consolidates technology for a better user experience and substantially lower costs. It includes: Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), malware defense, compliance policies, Data Loss Prevention (DLP), Browser Isolation, and 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

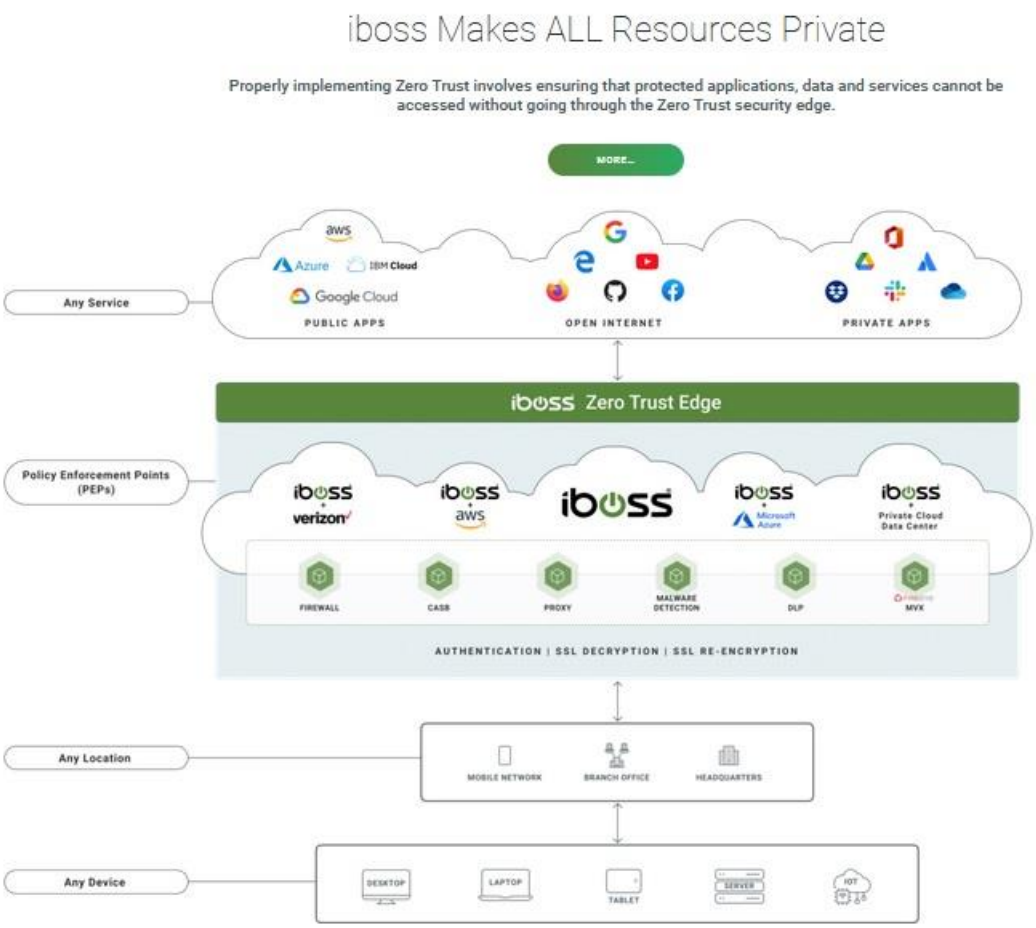
The iboss Zero Trust SSE inspects all content for malware, DLP, CASB, Compliance, Policies, and Logging. In addition to the iboss threat intelligence, the iboss platform leverages threat intel from other sources such as Verizon threat intel and applies that to every transaction.

A Complete Platform: ZTNA + Security Service Edge

Providing both Connectivity and Advanced SaaS Security Services



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 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.

To learn more, visit http://www.iboss.com.