iboss Secure Cloud Gateway
Certified Secure Test Report

12 September 2019

DR181218E

Miercom
www.miercom.com

Contents

1.0 Executive Summary

Traditional web gateways protect against threats crossing the network perimeter, blocking threats that could put 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 Secure Cloud Gateway (SCG) offers the flexible, scalable and reliable security that networks should have when the perimeter is not obvious. Using its proprietary engine, in conjunction with alliance engines from over 60 reputation feeds, this software provides advanced malware protection and web filtering for its users. No appliances are needed; this cloud-based solution has Software as a Service (SaaS) controls for internet security and compliance regulation of today's multi-cloud environment. This platform is fully integrable with third-party clouds, such as Microsoft Azure, by using globally operated, containerized cloud gateways to extend its fast and thorough protection for a high-quality user experience.

Unlike other web gateways, the iboss SCG can scan in-transit data within the cloud before it ever reaches the user or network. Its rich feature set successfully prevents complex malware, infections and data loss to save time and cost of 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 SCG platform automatically scales a collection of gateways to serve the bandwidth and capacity demands of any user, from any location.

When choosing a secure web gateway, the iboss SCG platform is a viable answer to typical and atypical network threats. iboss engaged Miercom to independently asses its SCG solution for its ability to secure network users in real-time against the latest threats by examining protective features, refined controls and user experience. Highlights from testing are as follows:

Key Findings of the iboss Secure Cloud Gateway

- **100% protection against advanced evasive techniques, advanced persistent threats, backdoor malware, remote access trojans and particularly ransomware – a costly malware affecting networks today**
- **99% security efficacy against complex, active malware samples and prevention against polymorphic zero-day threats**
- **99% average malware security efficacy, 22 percent higher than the average gateway tested with Miercom to date**
- **Successfully blocked user access to 100% of malicious, blacklisted URLs**

- **Countered data extraction of 100% of critical personal data categories – including credit card numbers, phone numbers, driver's licenses and social security numbers – over HTTP and HTTPS**
- **Extends security to web applications with granular application control for blocked URLs, categorized web browsing and integration with Microsoft CASB**
- **Streamlined setup with quick policy replication and distribution via template configuration allows for network-ready deployment**
- **Automated report generation and email alerts give robust administrative control using single pane of glass management**
- **Intuitive, in-depth event log, organizable by categories, domain and bandwidth with live bandwidth analysis for real-time view to network utilization**

The iboss Secure Cloud Gateway (SCG) 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 Product Tested

iboss Secure Cloud Gateway, *version 9.8.24.0*

CLOUD IS THE FUTURE

Cloud services are expected to grow 32 percent over the next five years, in comparison to a mere 5 percent for appliances. The iboss SCG platform provides elastic security for distributed workforces without needing cloud backups or appliances. No matter how much bandwidth or cloud capacity is used, appliances are not required – iboss has 100 data centers around the world to provide coverage and resources for any location.

For any given infrastructure with a typical cloud service, processing data with third-party applications like Azure, or a virtual LAN, would have to be pushed between the cloud and office users. But with iboss, the cloud service cohabits with these existing resources to eliminate data backhauling.

USER-BASED SECURITY

iboss secures user internet access, for any device and location. There is essentially no "perimeter" of the network with iboss, since it works natively with Internet-based applications. The remote user sees no difference web browsing on or off-site, and protection adapts to their network location as if they were always in the office. The unique approach of iboss is to provide granular user-based security, rather than the perimeter-based protection public cloud gateway security solutions offer.

Public gateways introduce security risks (e.g. SSL decryption private keys), have uncontrolled automatic update cycles, prevent extending IP address identify for easy third-party integration, lack geographic control and are limited by the vendor's cloud data size and capacity.

UNIQUE FUNCTIONALITY

When transitioning from appliances to the cloud, iboss presents the most seamless avenue to integrated security and functionality of the network infrastructure.

iboss distinguishes its cloud gateway platform from conventional appliance-based or cloud gateway architectures with a concept of global dedicated containerized cloud gateways that allow for:

- Cloud elasticity for an easily secured, distributed workforce
- Native expansion to third-party clouds for unified cloud security
- Regional regulatory compliance
- Elimination of appliance purchasing and maintenance
- Elimination of data backhaul
- Dedicated, non-shared capacity
- Extension of IP Identity to cloud for third-party vendors and integration
- Controlled upgrade cycles

MALWARE ANALYSIS

The iboss Secure Cloud Gateway (SCG) 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 network from local, remote or mobile endpoints.

Iboss protection makes use of three modules:

- Web Security Filtering
- Malware Defense
- Data Loss Prevention

A user can log 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 over 60 alliance engines – 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 extraction of personally identifiable information in real-time and from any geographical location.

2.2 Test Focus

Protective Features

- Malware Detection Engine
- URL Blacklisting

Refined Controls

- Application Control

User Experience

- Administrative Experience
- Logging (Reporting and Analytics)
- End Client Experience
- Scalability
- Compatibility

3.0 How We Did It

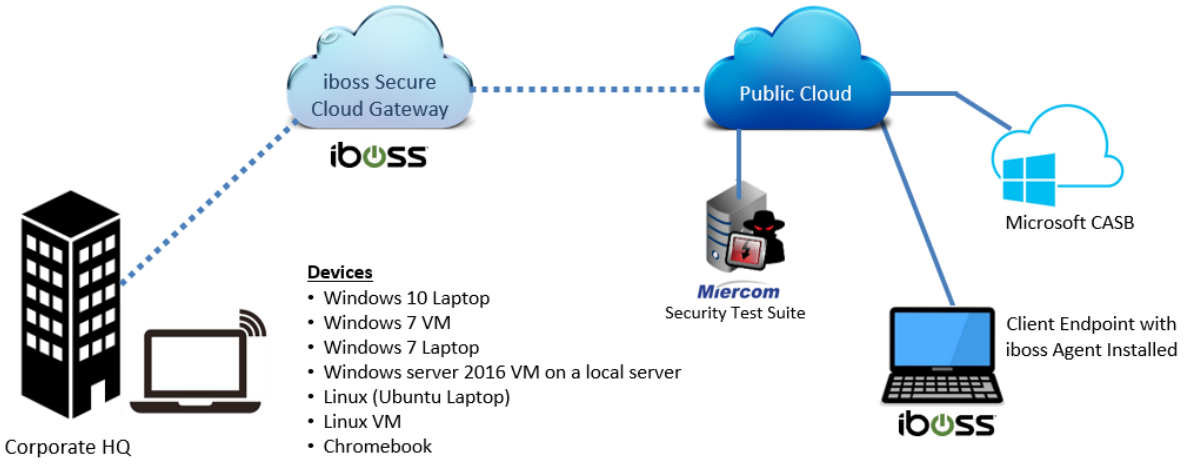
To test the functionality of the System Under Test (SUT), a custom-built network was created to simulate a real-world deployment. Traffic was generated and delivered through the network, along with malicious samples, to evaluate the ability of the SUT to detect, prevent and respond to threats.

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

3.1 Test Bed Setup

Our hands-on testing replicated a typical enterprise environment by using proprietary methods and tools to challenge the SUT. Each test is detailed in the remainder of this report.

Test Bed Diagram



Source: Miercom

The test bed above depicts the setup used to simulate an enterprise infrastructure with the iboss Secure Cloud Gateway platform deployed. The SUT was deployed in the cloud, between the corporate headquarters' network with its connected devices and the public cloud with the iboss agent installed. The Miercom Security Testing suite was connected to the public cloud, along with the Microsoft Cloud Access Security Broker (CASB) solution.

3.2 Test Tools

Source: Miercom

The test tools featured above are used for traffic and threat generation, real-time monitoring and capturing of network activity.

Ixia BreakingPoint optimizes security devices by simulating live security attacks and invasions. By sending a mixture of application traffic and malicious traffic, this tool determines the ability of the IPS and AV system to detect threats and remain resilient while exposed to vulnerabilities, worms and backdoors.

LiveAction Omnipeek captures network traffic and creates packet files for replay. Statistics can help monitor changes in real-time. By baselining normal activity, changes can be observed to analyze problem areas in the network.

4.0 Protective Features

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, malicious documents 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.

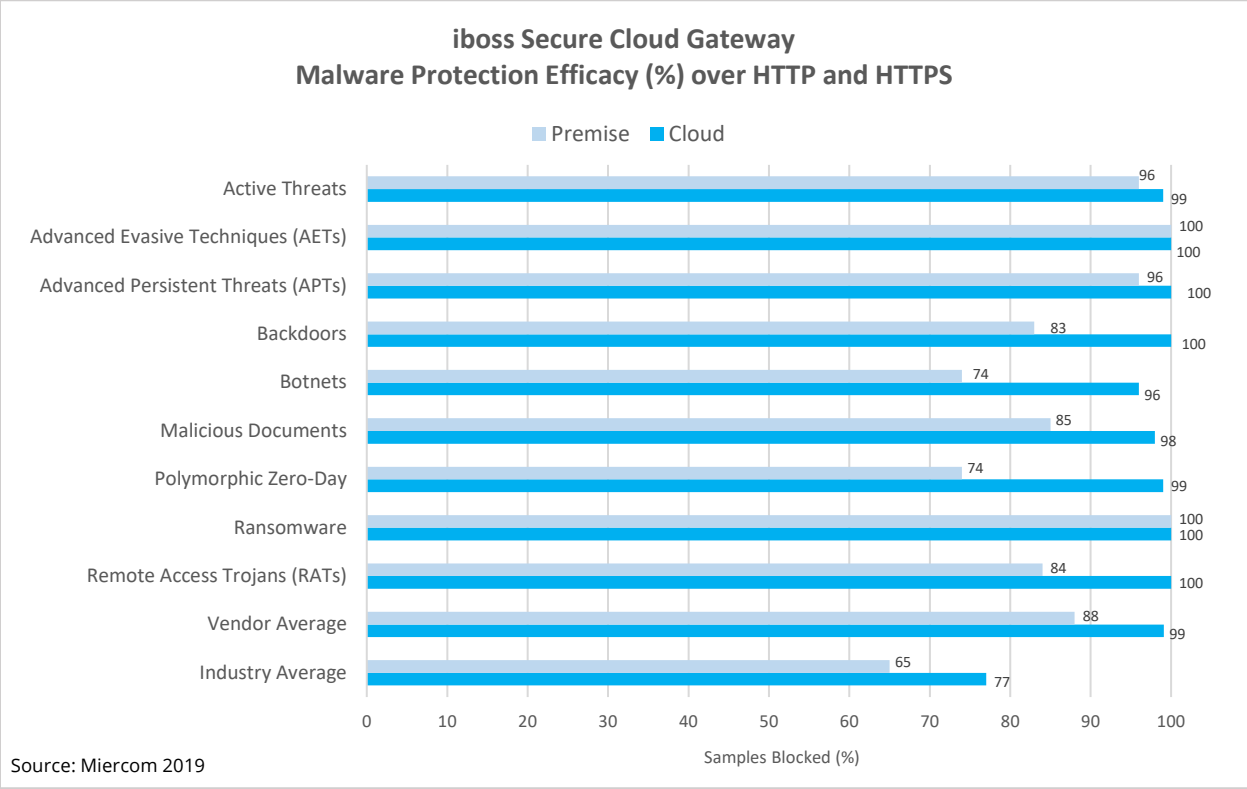
The SUT was an intermediary between untrusted and trusted zones of the simulated network. A simulated attack from the untrusted zone consisted of an attempted download of a malicious file. A successful block was logged when the simulated victim client cannot download the malware sample. Each file was attempted to be downloaded over both HTTP and HTTPS (TLS v1.2) connections.

Miercom Malware Samples

Miercom Malware Set
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 that delivers spam and Distributed Denial of Service (DDoS) attacks
Malicious Documents Mix of Microsoft and Adobe documents with macro viruses, APTs, worms
Remote Access Trojans (RATs) Trojans disguised as legitimate software which remotely control victim once activated

Advanced Threats
Active Threats Custom-crafted, constantly changing evasive malware
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
Polymorphic, Zero-Day Malware Constantly changing, difficult to detect; exploit known vulnerabilities

Results



Source: Miercom 2019

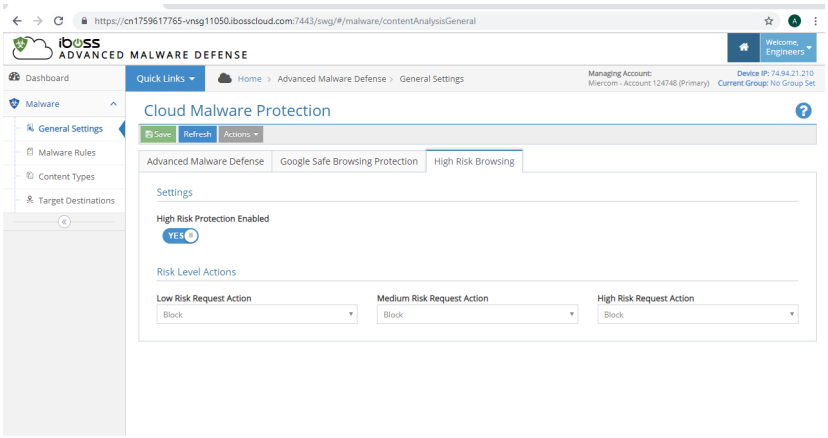
The iboss Secure Cloud Gateway platform detected 100 percent of ransomware – one of the most pervasive and current threats in the wild today. Iboss SCG blocked 99 and 100 percent of all malware categories using a combination of premise advanced signature blocking and cloud sandbox analysis. Samples were first analyzed using premise signature-based detection and then further examined in the cloud where they were subsequently blocked, resulting in higher efficacy scores. iboss blocked 22 percent more than the average vendor in its industry to date.

4.2 URL Blacklisting

Safe web-browsing is a crucial standard for secure web gateways. The first line of defense against harmful websites is an effective URL blacklist. Blacklisting ensures users are protected against malicious web locations that can open the network to attacks by making those IP addresses unreachable.

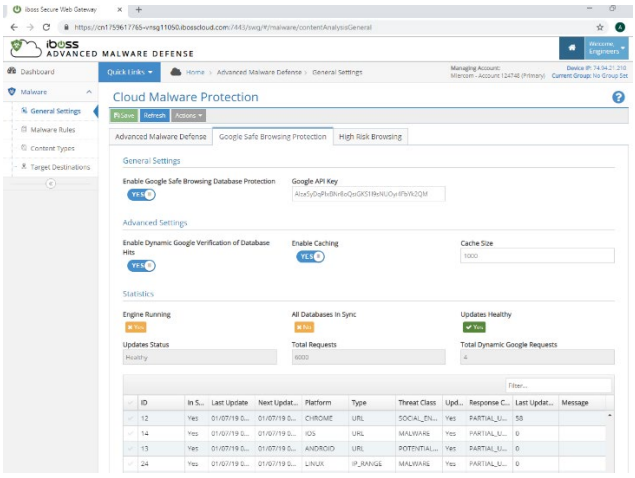
In this test case, a sample set of blacklisted URLs was used to determine the breadth of coverage when considering malicious web locations. The iboss SCG's Web Security settings were configured to block potentially malicious web locations. Two featured settings included High Risk Browsing and Google Safe Browsing as shown below.

High Risk Browsing Feature Enabled



Source: Miercom

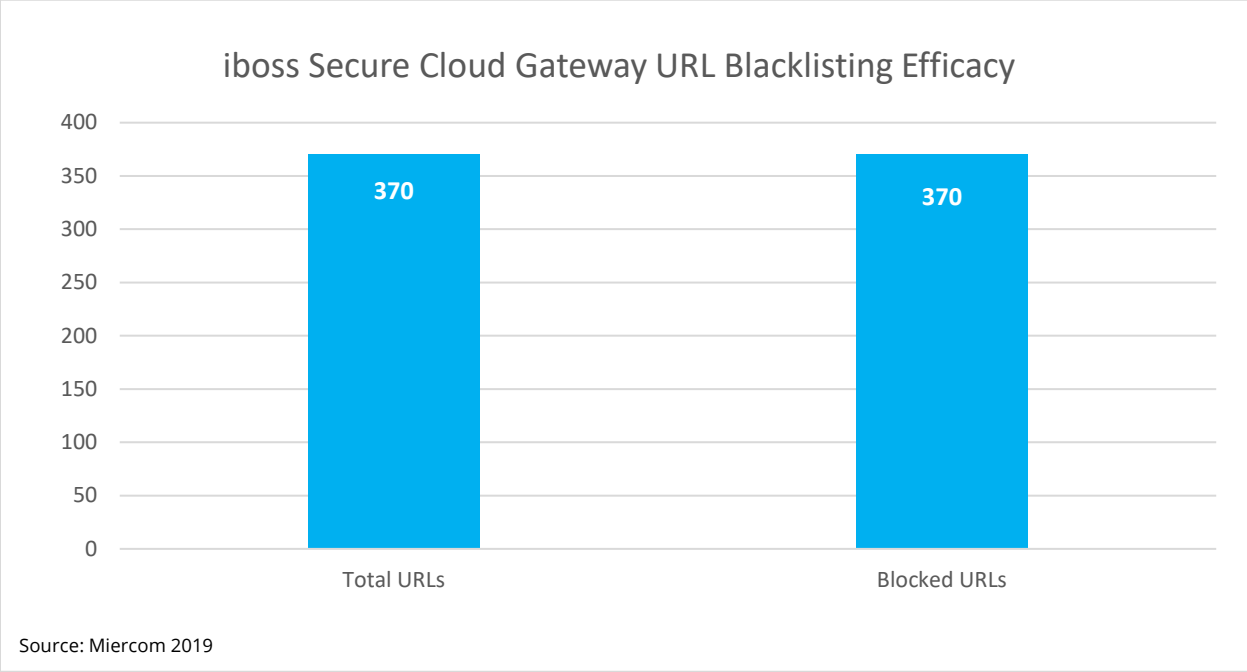
Google Safe Browsing Feature Enabled



Source: Miercom

Results

The iboss URL detection engine was shown to work well and prevents a user from accessing most malicious URLs assessed. In the event a user reaches a malicious web location, the malware detection engine assessed in the previous section will provide the next line of defense.



Source: Miercom 2019

A total of 370 URLs were reachable and expected to be blocked by the security product under test. The iboss Secure Cloud Gateway was able to prevent access to all of these malicious IPs –100 percent.

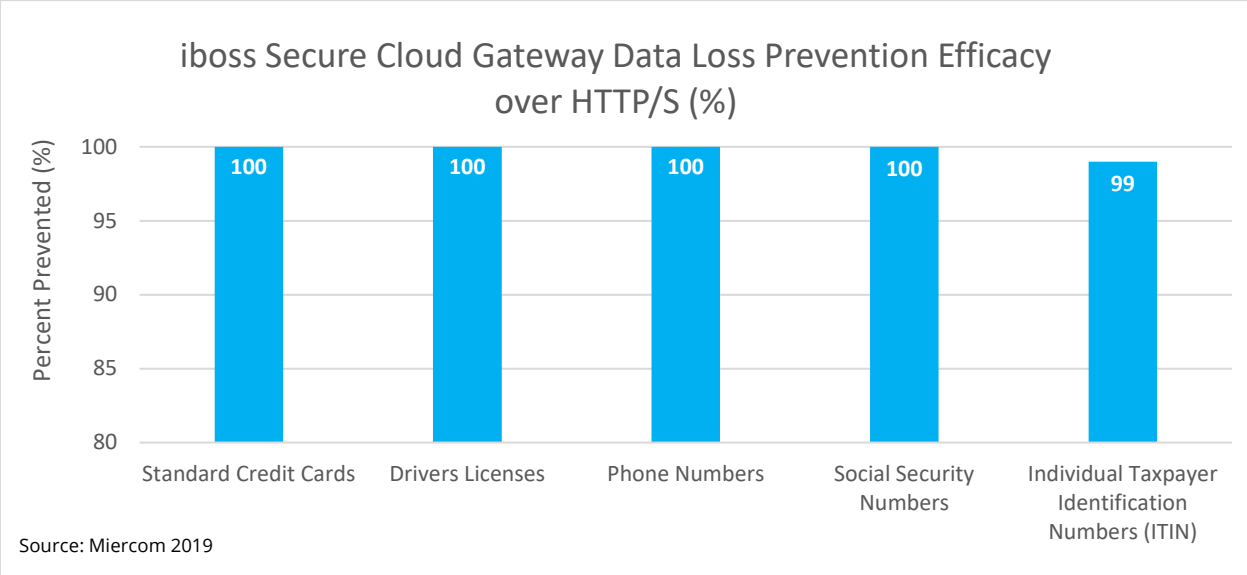
4.3 Data Loss Prevention

Data breaches cost millions of dollars each year, and this number is rising. Being able to detect and block possible data exfiltration events is a key capability for Data Loss Prevention (DLP) solutions. The iboss Secure Cloud Gateway platform was tested for this functionality by determining its ability to detect attempted extraction of credit card numbers, social security numbers, tax IDs, phone numbers and email addresses from the protected network. Exfiltration is attempted over HTTP and HTTPS protocols using text documents, Microsoft Word documents, SQL database files and archived documents.

An Apache server with HTTP and HTTPS POST commands was used to simulate breaches of a wide breadth of data formats and protocols to determine challenges for the iboss DLP engine. Thresholds were established within the administrative settings.

The iboss Secure Cloud Gateway constantly monitors to increase awareness of malware entering the network. Intelligence gained from monitoring is gathered to create a map for remediation. Correlation of threat events reveal a prioritized approach based on event severity. This allows the IT administrator to take action immediately.

Results



Source: Miercom 2019

The iboss Secure Cloud Gateway offers the option to prioritize remediation of events based on severity. The iboss platform immediately generated an alert after a suspicious, data breach event took place. These events were correctly categorized as malicious, quarantined and ultimately determined to be allowed or blocked based on administrative policies. Intelligence was accurate and effectively provided insight for immediate and useful remediating action.

5.0 Refined Controls

5.1 Application Control

Secure web gateways allow for propagation of security to web applications for granular control of enabling/disabling functionality, user access and antimalware policies.

A standalone iboss deployment has the capability to manually block applications such as Facebook, Twitter, YouTube, Pinterest, or Spotify. The administrator can also manually add signatures for applications that are to be blacklisted. The results of the built-in feature testing are shown in the table below. Additionally, iboss has compatibility with industry partners that can make this feature set comprehensive and even more simplistic for the administrator.

In this test case, Miercom wanted to assess the capability of the iboss SCG when incorporated with Microsoft's CASB. iboss leverages the over 16,000 predefined applications from the Microsoft CASB solution in order to provide extensive administrative control. Miercom successfully observed the iboss solution import the unsanctioned application information and successfully block the chosen applications.

In this test configuration, Miercom engineers configured CASB to apply a policy to automatically "un-sanction" applications that are below a score of 5 in the Microsoft CASB solution. Application information is sent from the iboss SCG to the Microsoft CASB and upon discovery of the application, the ruleset is applied. Miercom observed this integration result in rules automatically applied in the SCG.

The applications used to quality this capability included: Facebook, Reddit, Twitter, Imgur, Skype, YouTube, Spotify and Pinterest. This range of applications demonstrate the highly configurable capabilities provided by the iboss SCG product.

Results

Procedure	Application Control	Observation	Result
URL Blocking	**Blocked URLs:** https://facebook.com https://cnn.com https://github.com https://httpstatus.io https://www.iwf.org.uk	Blocked instantly Once cleared from blocked list, the website was immediately available.	**Pass**
Web Control by Category	**Categories:** Gambling Dating sites Malware content	Sites were blocked, and the landing page was loaded with blocked page	**Pass**

Application Control by Application Management	**Jabber Instant Messenger:** Created two accounts @jabber.at	Although trying to block the jabber Instant Messenger, we were unable to stop calls between the two jabber accounts	**Pass***
Application Control by CASB Account	**CASB Account:** CASB account was made through a Microsoft account and was easily incorporated through the CASB API.	Application control was done through the CASB. iboss was able to point correctly. All applications were blocked.	**Pass**

** Successfully blocked Jabber application through GRE tunnel but does not block with current version of agent.*

6.0 User Experience

This section reviews user experience for the following:

- Administrative
- Logging: Reporting and Analytics
- End Client Experience
- Scalability
- Compatibility

6.1 Administrative Experience

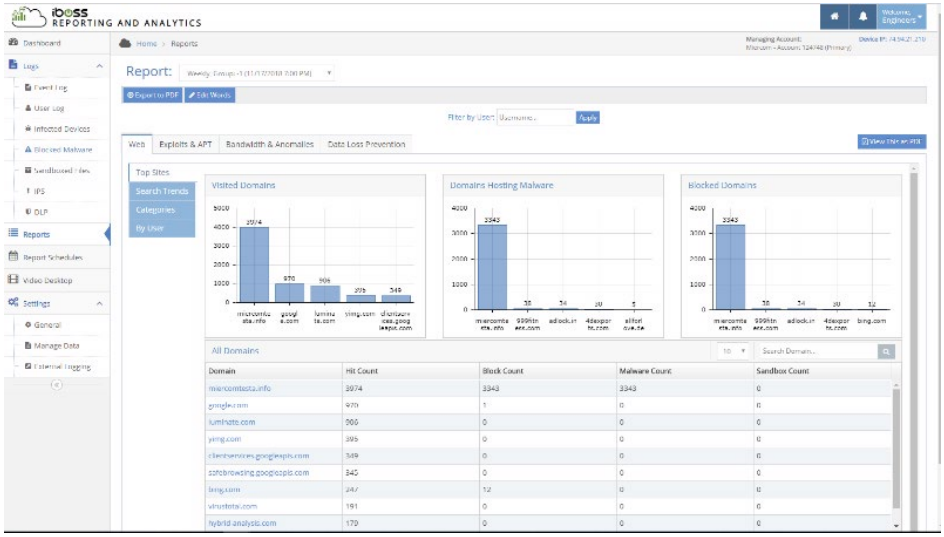
The iboss SCG is highly configurable with a simplistic interface. Its centralized tile structure allows the administrator to effectively navigate into subcategories for focused setting alterations and provides an intuitive division of settings and features for quick navigation to the required setup pages.

Cloud management allows for ease of use from any location.

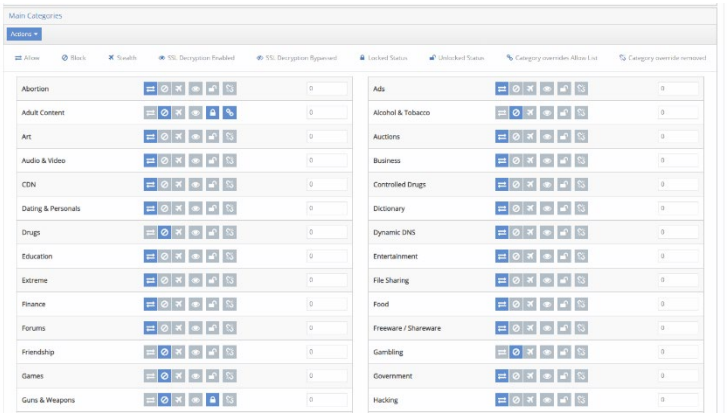
Email alerts: Miercom assessed the email alert capabilities provided by the iboss SCG. This test found that alerts are configured for three different categories: keyword violations, threshold Monitoring violations, and automated report generation.

Keyword configuration: This feature allows administrators to receive alerts when a user is continuously searching for specific keywords. This feature allows for a custom threshold to be set and can provide useful automated feedback to administrators if a user is continuously researching items such as bombs, drugs or murder.

Automated Report Generation: Automated report generation was configured to send daily reports. These reports showed statistical details such as top domains blocked, DLP data, and active infected clients over the 24-hour period prior to report generation.



Ease of configuration:



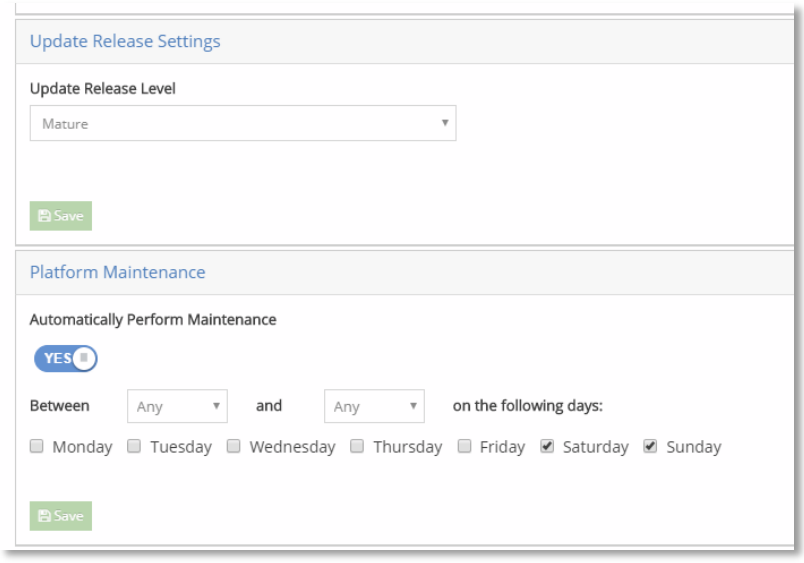
Miercom investigated the import of a policy template – like a standard template a customer receives as a first step toward configuration of the SCG environment.

Upon successful import of the policy template to an assigned group, the pre-configured template settings were automatically applied to all applicable configurations. This automatic configuration option allows an administrator to quickly replicate or distribute a policy to, and from, other security groups. After the template is imported, the administrator can navigate to the pages and further customize any rules that require additional or less strict security settings.

Other noteworthy features observed during assessment of the administrative experience:

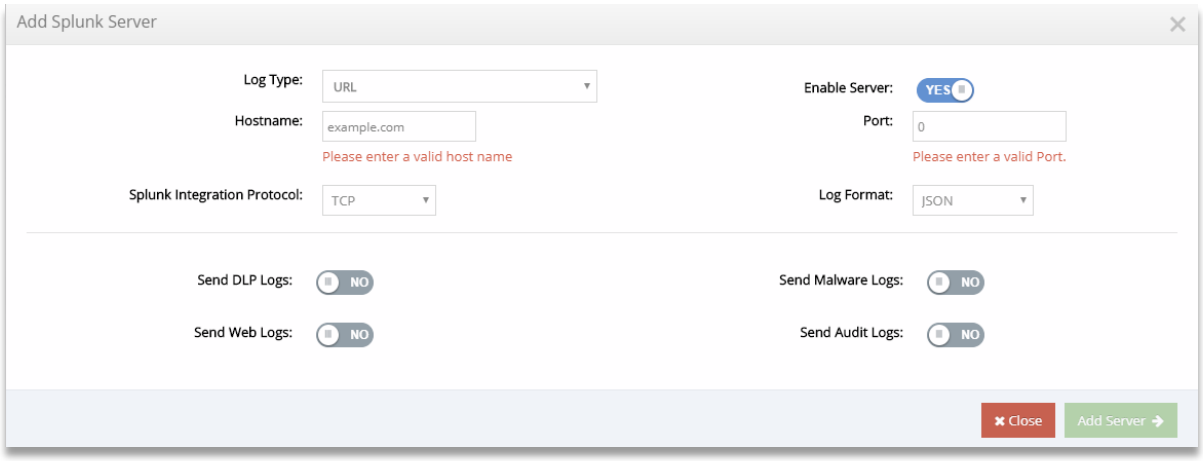
Single pane of glass management: The iboss SCG utilizes a single landing page with categorized tiles serving as links to specific configuration settings. This centralized starting point serves as a useful base for the start of any administrative action. The intuitive categories allow a user to dig down into settings that relate to categories such as “Advanced Malware Defense” or “Reporting and Analytics”.

Manual option for scheduling updates or maintenance: Avoid downtime during productive hours.



iboss offers the ability to manually schedule update and maintenance for a better user experience.

Option for SIEM integration was available, as shown below with the Spunk Integration tool. The SIEM can be streamed directly – with no need for a virtual server. Some competitors require the use of a streaming log server and service, providing a host in the cloud which must be maintained. Unlike iboss SCG, using a streaming server is not a true SaaS offering. Features such as external logging to SIEM and data export from the iboss Cloud reports are simple, and they do not require the use or management of a separate streaming server. iboss allows direct integration with Cloud Splunk and other SIEMs via SYSLOG, FTP, SFTP with TCP/SSL communications, along with the ability to customize Extended Log File Format (ELLF), where fields can be specified by order and content sent to external loggers.



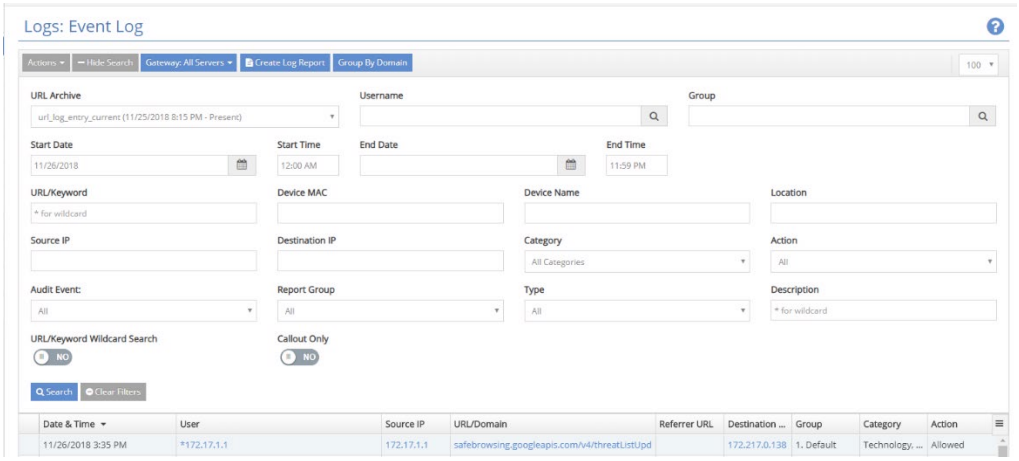
6.2 Logging: Reporting and Analytics

The logs contain the basic security information and are successfully filtered in chronological order. A customizable view of these logs is available, based on categories, which allow administrators with an organized view of events. Logs are mainly focused on web information (categories, domains, bandwidth), and live bandwidth analysis was particularly interesting for its ability to show real-time network utilization. Threats are also present in the incident response page.

The iboss reports and analytics page allows for a smooth end user experience; an easy overview of the system health is readily obtained. Tabs like "Incident Response Center" allow for quick identification of immediate threats and further information is available via a link inside the tabular display.

The event log gives an in-depth overview of both allowed and blocked events seen by the SCG. These events can be filtered with the many criteria options available using a search feature at the top of the page. The search can be based on detailed criteria ranging from specific time frames to device MAC, or even location.

The reporting and analytics section also contains further informative breakdowns – by user, sandboxed files, IPS engine and possible DLP violations.



The interface allows for an export of logs to provide the same level of detail available via email, as needed by the system administrator. Log exports can be scheduled for further automation to ease some of the administrative burden.

6.3 End Client Experience

A single agent install allows the product to work from any location in which internet is available. Agent install on Windows is particularly simple, making for an easy setup with no errors.

From a client perspective, the iboss SCG application is similar to a web proxy. The application runs in the background and only becomes visible to the end user when content is blocked.

6.4 Scalability

Traditional gateways require multiple applications to accomplish what multi-cloud access can do. They are also limited by the network perimeter. But the cloud-based approach gives scalability and universal access to users, giving the secure web gateway more coverage and flexibility.

As a fully SaaS solution that is hosted in the cloud, the iboss SCG platform can be dynamically managed in order to expand with network size.

Active Directory (AD) Integration

The iboss SCG can integrate with an AD instance with a plugin provided by iboss, which uniquely does not require AD Federation Services (ADFS) or domain resources to the cloud. The iboss cloud connectors automatically associate the username to the data being processed and logged, as well as correlating directory groups to match security groups within the platform. All associations are made without exposing any AD servers, opening firewalls or relying on ADFS resources.

Deployment

Chromebook is one of iboss' most mature deployment scenarios. This deployment makes use of Google's G Suite. The Chromebook integration is a fantastically simple way to maintain large groups. The integration of iboss requires minimal administrative configuration and will automatically be applied to new users placed in the applicable groups. Upon login to a new device, the administrative settings automatically install the iboss application and begin routing traffic through the protected web gateway.

Okta Integration for Third-Party Authentication

The ability for iboss to integrate with third-party authentication providers allows for seamless scalability when adding new users or expanding the company infrastructure.

The tested integration involves a remote client accessing an internal intranet location utilizing SAML authentication and has IP restrictions that will only allow authentication via the static IP provided by the iboss SCG product.

6.5 Compatibility

This test item demonstrates the integration of the iboss SCG with Windows, Chromebook, and Linux clients. Because the SCG is entirely hosted in the cloud and is a pure SaaS solution, the pillar of the compatibility with each product is the capability to route network traffic through the iboss SCG. The redirection of traffic is a common configuration requirement on corporate devices to ensure continuous protection from all access locations.

With the iboss SCG, cloud migration can be seamless while still maintaining functionality. The SCG is shown to be easily integrated with each of these products:

Windows
Windows deployments are seamless when using the iboss application. The install is quick and effective; immediately routing traffic through the iboss SCG cloud.

Mac
Mac deployments were very simple with the iboss application; installation was quick and straightforward.

Chromebook
Chromebook deployment is extremely easy. Once the application is assigned as a mandatory download, and the settings are properly configured, a new user can log into a fresh Chromebook with the application automatically installed to protect the user's web browsing.

Linux
The Linux endpoint routes traffic through the cloud utilizing a standard OpenVPN connection. A configuration can be provided by the iboss support team for the applicable Linux distribution. The end user imports the configuration file and enables the VPN connection to enable the secure web gateway features.

Microsoft CASB
Users with pre-existing Microsoft CASB accounts can integrate the iboss SCG with a URL and an API key from the Microsoft CASB interface. After this is complete, the SCG will import the unsanctioned application information and apply it to the policy settings of the SCG.

While integration is possible, it should be noted that iboss SCG can see and apply policies (allow/block) to applications by default – even without Microsoft CASB. It is not a requirement to have CASB integration to block these applications.

Integration provides, not only CASB visibility for data resting in the cloud but, information for all application data in motion to CASB. It also allows for in-depth Cloud App discovery and bi-directional communication between the two platforms for an easy toggling of unsanctioned applications from CASB, and for iboss to quickly apply policies around it. Again, like integration, this visibility isn't a requirement to enforce application policy via the iboss SCG.

About Miercom

Miercom has published hundreds of network product analyses 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 analyses, 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 for product usability and performance.

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 relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 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 own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.