Data Sheet

Reporting & Analytics

iboss™
THE DISTRIBUTED GATEWAY PLATFORM

For Enhanced Malware Detection and Rapid Breach Response

Key Features & Capabilities

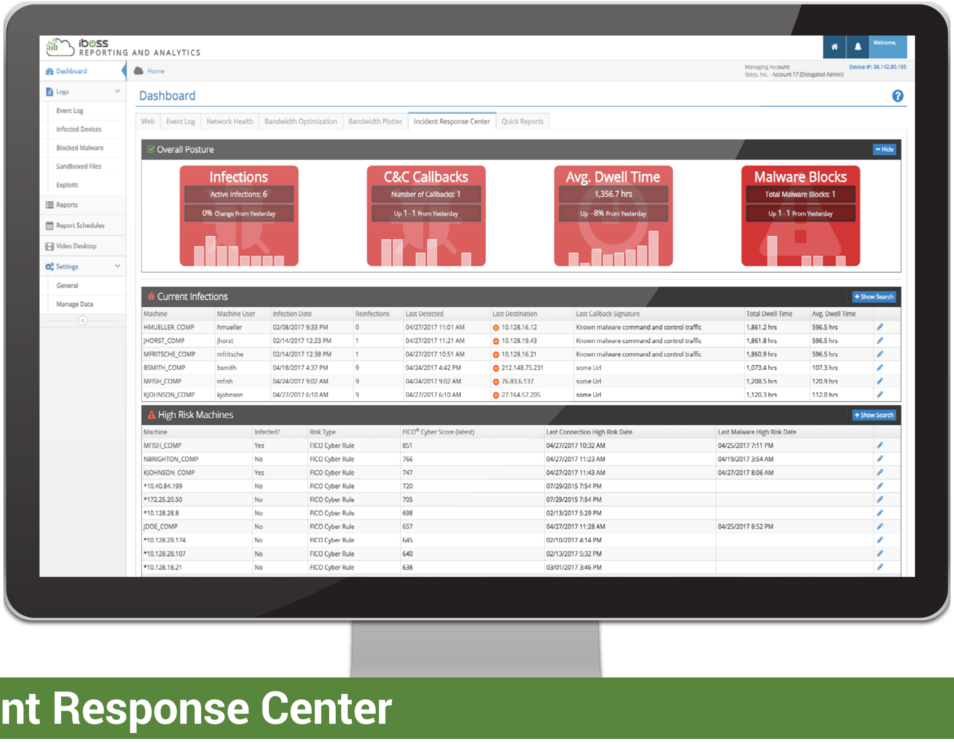
- Incident Response Center
- Forensic Data with SIEM Integration
- Live Bandwidth Activity Feed
- Real-time Threat and Risk Intelligence
- Video Desktop Recorder

The iboss Distributed Gateway Platform offers a Reporting and Analytics console which provides granular visibility into all Internet traffic moving across an organization's network. With packet-level detail, the Reporting and Analytics console gives IT and network operations teams the real-time, actionable intelligence they need to quickly identify and mitigate infections caused by web-borne malware. It also identifies high-risk user behaviors, enabling administrators or IT teams to take action to eliminate the risk and prevent data loss.

The Reporting and Analytics console features are integrated across the iboss Distributed Gateway Platform, and are included as standard functionality in all subscription packages. The unique features included in the console enable administrators and IT staff to effortlessly switch between network-wide views to 360-degree historical and real-time views of each user, including their web activity, applications, bandwidth consumption, infections, data loss risk and more.

iboss Distributed Gateway Platform Unique Node-Based Architecture

The iboss Distributed Gateway Platform is specifically designed to meet the cybersecurity needs of distributed organizations – but it does so in a completely different way. Built for the cloud, the iboss Distributed Gateway Platform can defend today's complex and decentralized networks, and the branch offices, remote locations, and mobile users that depend on them. The iboss Distributed Gateway Platform also provides the flexibility required to drop-in and replace existing on-prem systems, allowing organizations to transition to the cloud smoothly, at their own pace, without the need to re-architect their existing networks.



Managing Account:
iboss, Inc. - Account 17 (Delegated Admin)

Device IP: 38.142.80.195

Dashboard

Overall Posture

Infections
Active Infections: 6
0% Change From Yesterday

C&C Callbacks
Number of Callbacks: 1
Up 1 1 From Yesterday

Avg. Dwell Time
1,356.7 hrs
Up 8% From Yesterday

Malware Blocks
Total Malware Blocks: 1
Up 1 1 From Yesterday

Current Infections

Machine	Machine User	Infection Date	Reinfections	Last Detected	Last Destination	Last Callback Signature	Total Dwell Time	Avg. Dwell Time	
HMUELLER_COMP	hmueller	02/08/2017 9:33 PM	0	04/27/2017 11:01 AM	10.128.16.12	Known malware command and control traffic	1,861.2 hrs	596.5 hrs	✎
JHORST_COMP	jhorst	02/14/2017 12:23 PM	1	04/27/2017 11:21 AM	10.128.19.43	Known malware command and control traffic	1,861.8 hrs	596.5 hrs	✎
MFRITSCHE_COMP	mfritsche	02/14/2017 12:38 PM	1	04/27/2017 10:51 AM	10.128.16.21	Known malware command and control traffic	1,860.9 hrs	596.5 hrs	✎
BSMITH_COMP	bsmith	04/18/2017 4:37 PM	9	04/24/2017 4:42 PM	212.148.75.231	some Url	1,073.4 hrs	107.3 hrs	✎
MFISH_COMP	mfish	04/24/2017 9:02 AM	9	04/24/2017 9:02 AM	76.83.6.137	some Url	1,208.5 hrs	120.9 hrs	✎
KJOHNSON_COMP	kjohnson	04/27/2017 6:10 AM	9	04/27/2017 6:10 AM	27.164.57.205	some Url	1,120.3 hrs	112.0 hrs	✎

High Risk Machines

Machine	Infected?	Risk Type	FICO® Cyber Score (latest)	Last Connection High Risk Date	Last Malware High Risk Date	
MFISH_COMP	Yes	FICO Cyber Rule	851	04/27/2017 10:32 AM	04/25/2017 7:11 PM	✎
NBRIGHTON_COMP	No	FICO Cyber Rule	766	04/27/2017 11:23 AM	04/19/2017 3:54 AM	✎
KJOHNSON_COMP	Yes	FICO Cyber Rule	747	04/27/2017 11:43 AM	04/27/2017 8:06 AM	✎
*10.40.84.199	No	FICO Cyber Rule	720	07/29/2015 7:54 PM		✎
*172.25.20.50	No	FICO Cyber Rule	705	07/29/2015 7:54 PM		✎
*10.128.28.8	No	FICO Cyber Rule	698	02/13/2017 5:29 PM		✎
JDOE_COMP	No	FICO Cyber Rule	657	04/27/2017 11:28 AM	04/25/2017 8:52 PM	✎
*10.128.28.174	No	FICO Cyber Rule	645	02/10/2017 4:14 PM		✎
*10.128.28.107	No	FICO Cyber Rule	640	02/13/2017 5:32 PM		✎
*10.128.18.21	No	FICO Cyber Rule	638	03/01/2017 3:46 PM		✎

Incident Response Center

The Reporting and Analytics console includes the Incident Response Center, which provides instant and comprehensive visibility into threats and infections, backed by real-time threat intelligence crowdsourced from millions of endpoints worldwide. The Incident Response Center correlates this data across a wide range of parameters, instantly delivering actionable forensic intelligence on zero-day threats and evasive malware.

Unlike other products that overwhelm teams with a flood of redundant alerts from a single malware event, the Incident Response Center eliminates alert ‘noise’ by greatly reducing false positives and cascading alerts. It accomplishes this by compiling and correlating threat intelligence to enable prioritized alerting. This dashboard also helps teams to focus and expedite their responses to malware episodes by providing highly detailed threat and attack information. For example, it shows where malware first infiltrated the network, what users and devices are involved, and where the attack has spread.

Key Capabilities Include:

- Consolidating threat intelligence and dynamically correlating outbreaks to shorten remediation times
- Correlating alert information to individual users in the directory or to specific machines, along with a snapshot of global outbreak histories, enabling more effective responses
- Leveraging crowdsourced global threat intelligence to deliver the latest malware infection information
- Eliminating noise by reducing false positives and redundant alerts
- Aggregating data from more than 50 separate malware engines for comprehensive threat intelligence
- Monitoring and mapping infection callbacks to mitigate data loss
- Identifying IP aliases and malicious hosted files to prevent future attacks

Forensic Data with SIEM Integration

The Reporting and Analytics console indexes data logs dynamically, and can store unlimited amounts of historical threat and malware activity data. It also combines that data with event management functions to deliver integrated security information and event management (SIEM) capabilities that help organizations understand and act on threats faster.

With the SIEM functionality and native Splunk integration, account administrators can:

- Gain visibility into usage across the organization, or drill-down for packet-level details on a single user
- Generate reports for all inbound and outbound ports, applications, and IP addresses
- Create analytical comparisons on date ranges for bandwidth or user activities
- Track and log activities on search engines, blogs, videos and more for a concise list of sites and search terms used

Live Bandwidth Activity Feed

The Reporting and Analytics console's Live Bandwidth Dashboard is designed to help safeguard bandwidth availability and prevent disruption of key services and applications. It provides visibility into and control over all bandwidth consumption across an organization. Features including geotagging, reverse-geo-mapping of IP addresses, and a global map overview provide instant insight into the status of network resources to help IT and network operations teams resolve problems faster.

The dynamic bandwidth plotter provides a heat map that enables teams to track potential threats by:

- ✓ Top bandwidth consumers by user and IP address
- ✓ Total bandwidth consumption on the network
- ✓ Connections, locations, and individual packets or data usage

The bandwidth plotter is integrated into the Bandwidth Optimization feature within the Distributed Gateway Platform. It allows organizations to optimize network performance and ensures critical SaaS services and mobile device usage are never at risk.

Real-time Threat & Risk Intelligence

The Reporting and Analytics console displays a Live Threat Dashboard that provides immediate insight into threats, suspicious events, and liability risks that can result in acceptable use policy violations, compliance infractions, data loss or costly litigation. Delivering snapshots of trouble spots before they cause serious damage, it enables instant visibility into:

- User activity to pinpoint the most active users and active violators
- Network violations, current threats and trends
- Suspicious events, security risks and liabilities

Video Desktop Recorder

Also integrated into the Reporting and Analytics console is the Video Desktop Recorder. This tool provides actionable intelligence on suspicious events by recording user activity and alerting administrators when policy violations are detected. Recordings are activated by customer-defined triggers. Once activated, this feature can monitor, record and control up to 10 desktops per monitor simultaneously. The Video Desktop Recorder is a patented feature that no other solution offers.

About iboss

iboss has created the first and only Distributed Gateway Platform specifically designed to solve the challenge of securing distributed organizations. Built for the cloud, iboss leverages an elastic, node-based architecture that provides advanced security for today's decentralized organizations and scales to meet the ever-increasing bandwidth needs of tomorrow. The iboss Distributed Gateway Platform is backed by more than 100 patents and protects over 4,000 organizations worldwide, making iboss one of the fastest growing cybersecurity companies in the world.

To learn more, visit www.iboss.com or contact iboss at sales@iboss.com