iboss

Detailed Logging and Reporting

The iboss cloud includes detailed logging and reporting that provides clear visibility into cloud use to reduce infections and gain insight regardless of user location

The platform includes detailed logs that include username, device name, group, source IP address, URL, timestamp and a large number of attributes needed to correlate cloud use information to specific users and devices. This allows IT administrators to quickly locate problems such as infected devices or risky users which results in faster remediation and less downtime. The logs are stored in iboss cloud and automatically backed up to ensure data is always available when needed while eliminating the need for tape backup to preserve web logs.

In addition, detailed drill down reports contain information that can be presented to executives, human resources, and IT security teams on demand or on a schedule. The reports can be customized including what content should be included in the report. Customized content can include top users by activity, infections, blocked malware in addition to dozens of other specific data. Reports are downloadable or can be sent via email in PDF format either on demand or on a schedule.

Reporting data can be streamed directly from iboss cloud to any external SIEM or logging database to ensure existing logging databases are leveraged. This includes preserving existing processes and teams already designed around existing SIEM platforms. Since the iboss cloud protects user Internet access from anywhere, including out of the office, security operations teams will gain additional visibility into activity typically not available when users are outside of the office.

Detailed log events including username, device name and timestamp

Generate PDF and drill-down reports from pre-built templates for Executives, IT, and HR

Generate reports on-demand or on a schedule

Stream data from the iboss cloud to existing SIEMs and SOC

Detailed log events including username, device name and timestamp

The iboss cloud will generate log events for user cloud activity regardless of location. This includes data from users in and out of the office since the iboss cloud protects users wherever they roam. The log events are detailed and includes a large number of fields including username, device name, URL and timestamps. They can be searched with very specific criteria to locate specific events and incidents.

Log events are stored in the cloud eliminating the need for expensive storage and backup systems. Logs are automatically backed up within iboss cloud to ensure availability when needed.
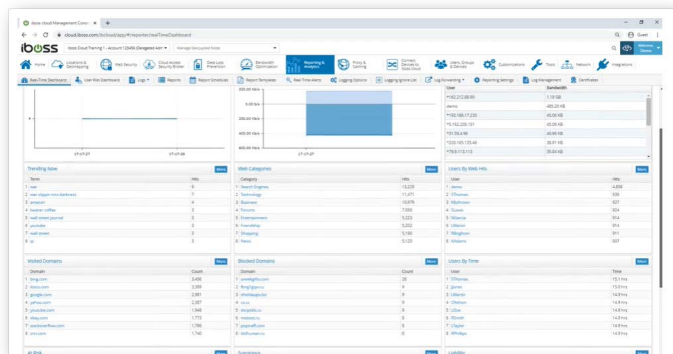
Generate PDF and drill-down reports from pre-built templates for Executives, IT, and HR

Drill down reports can be generated from pre-defined templates or customized to include information specific to executives, IT, or HR. This reduces time to generate the information needed when requests come in from different departments such as HR or legal.

In addition, drill down reports can be completely customized to include information such as time use, activity, infections, data loss and Internet use costs. This ensures the information is presented in format that is easy to understand for technical and non-technical audiences.
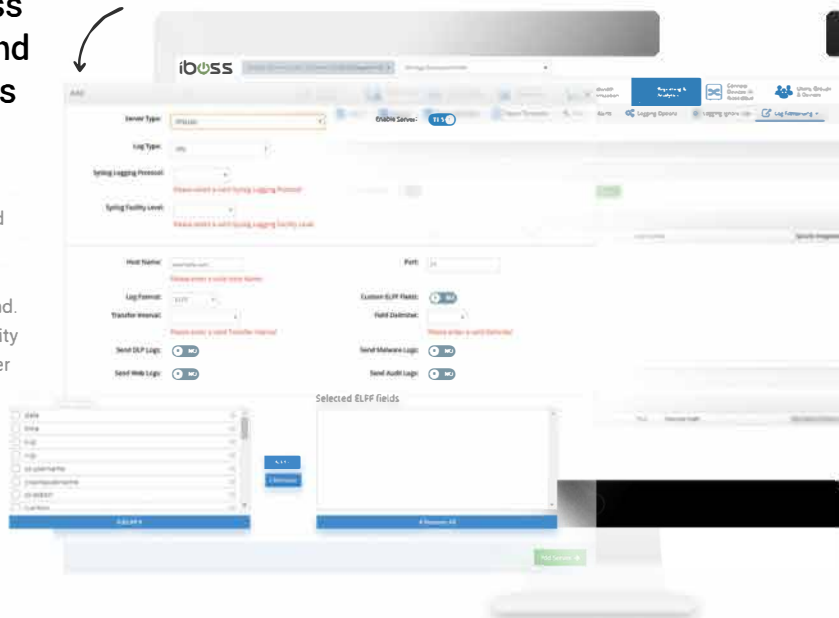
Generate reports on-demand or on a schedule

Reports can be scheduled on-demand or run on a schedule. Scheduling includes day and time as well as specific recipients. Different types of reports can be scheduled including drill down reports and log event reports that include time stamp level details. All reporting and scheduling is performed from the admin console and runs in the cloud eliminating the need to manage infrastructure.
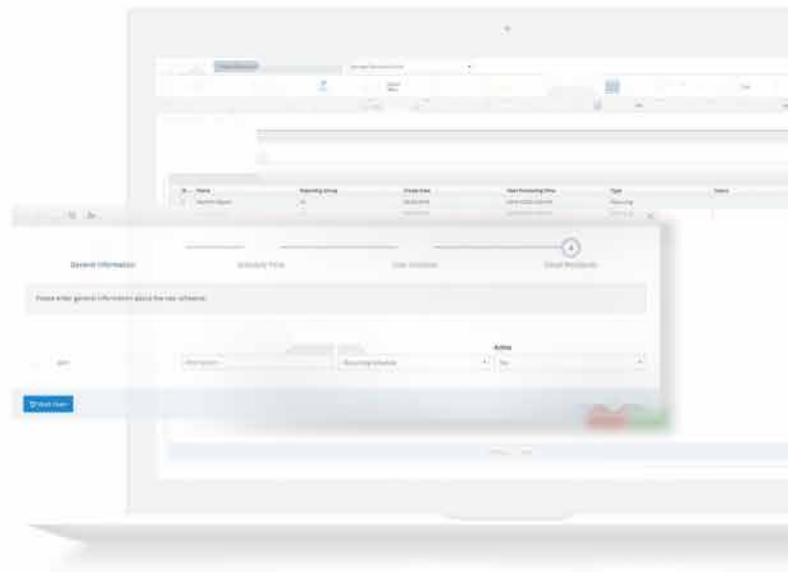
Stream data from the iboss cloud to existing SIEMs and Security Operation Centers

Add as many log forwarding entries to forward logs to multiple destinations simultaneously.

Any log event the iboss cloud generates can be sent to any external system including SIEMs and Security Operation Centers. This includes cloud activity events from users within the network perimeter, such as the office, or users on the road. This enriches the information available to security teams to eliminate blind spots and provide faster remediation when issues occur.

Add and adjust forwarded log fields so that they match the receiving SIEM format

Buy Now

The iboss cloud can secure user Internet access on any device, from any location, in the cloud. Best of all, you can start using it immediately to protect your users instantly.

What you get

- In the cloud Internet security
- Advanced Internet malware protection that follows users
- Advanced cloud and SaaS controls
- Web filtering and compliance controls
- Internet security for in-office users without appliances
- Branch office Internet security without data backhaul
- And a lot more...

Contact Us

Get in touch with a technical specialist for a live demo.

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEIA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

CONTACT SUPPORT

Support Overview
Open a Ticket

North America Support:
877-742-6832 X3
support.na@ibosscloud.com

LATAM Support:
+52 (55) 41696270
support.latam@ibosscloud.com

EMEIA Support:
+44 (0) 203 7908289
support.emeia@ibosscloud.com

APAC Support:
+63 (45) 4571057
support.apac@ibosscloud.com

CONTACT SALES

Request Demo
Request Information

North America Sales:
877-742-6832 X1
Contact local distributor or:
sales@iboss.com

International Sales:
858-568-7051 X1
Contact local distributor or:
sales@iboss.com

EMEIA Sales:
+44 20 3884 0360
Contact local distributor or:
emeia@iboss.com

iboss