Detailed and Granular Internet Activity Reporting

The iboss cloud provides the most advanced and detailed Internet activity reporting for identifying high risk users, lost productivity and infected devices.

Internet Activity Reporting Overview

The iboss cloud provides deep, granular and detailed reporting to identify high risk users, lost productivity, infected devices, and risky Internet access quickly. The advanced reporting capabilities within iboss cloud can instantly deliver the following benefits:

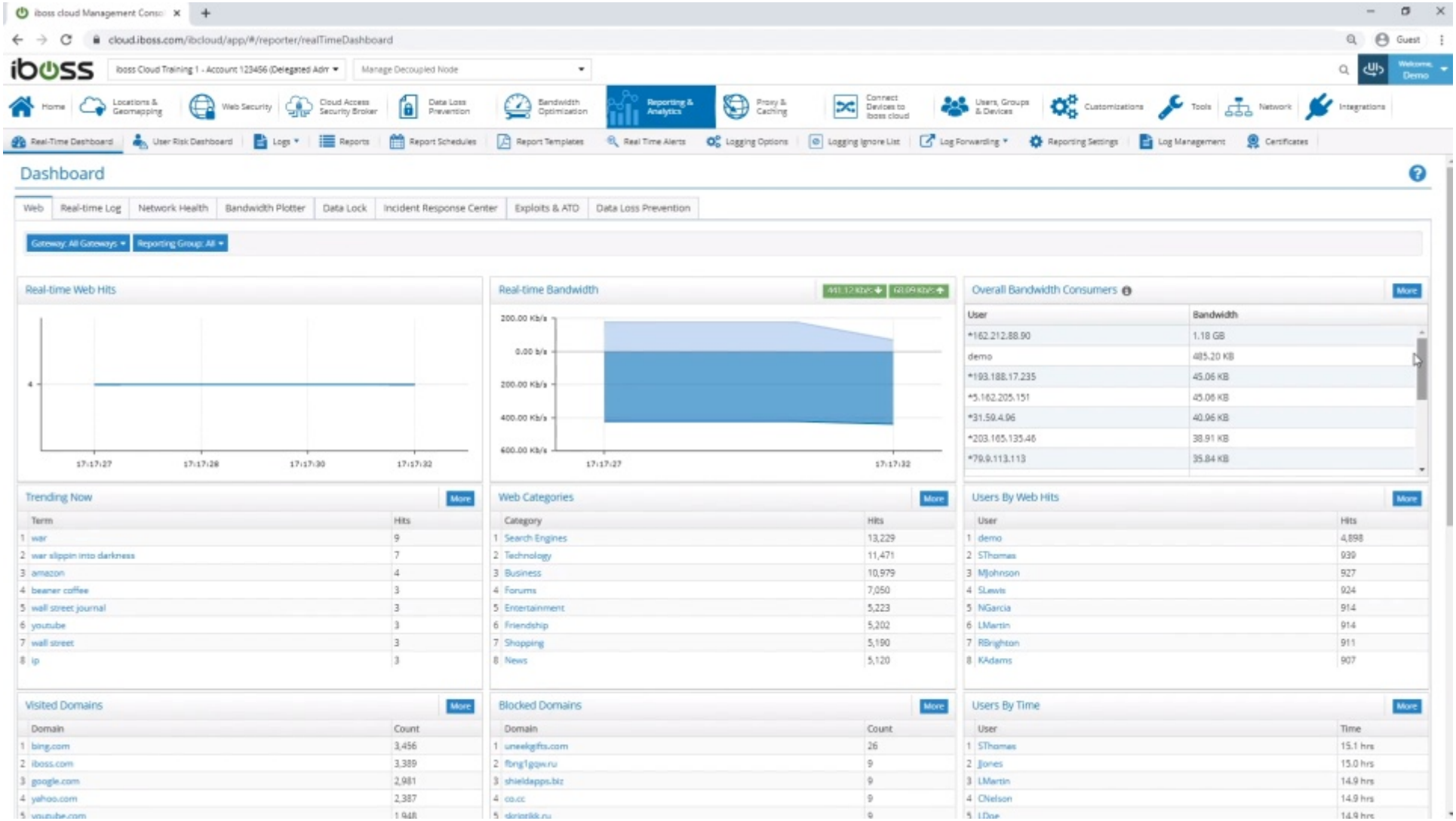
- Associate Internet activity to users by username as the iboss cloud automatically associates usernames to every Internet access
- View the full URL, not just domain names, for Internet accesses to understand exactly what activities are occurring throughout the organization
- Gain visibility into full URLs within encrypted HTTPS traffic which is traditionally missing from typical Internet security solutions
- Gain visibility into user activities on organization owned devices at all times, including when users are mobile and outside of the four walls of the traditional network perimeter
- Detailed logs contain all of the necessary information to re-mediate issues quickly including username, source IP, URL, destination IP, categories and timestamps
- Reporting AI automatically extracts the most important information to immediately show high risk users, high risk search terms and information of interest
- Drill down reports that are interactive and can be used for investigations or on demand report requests
- Scheduled reporting that can be configured to automatically send information targeted to Executives, HR, Superintendents, and other administrators
- Real-time dashboards including bandwidth, network connections, top destination and more
- Real-time alerts when key search terms are hit by any user to respond quickly to very high risk behavior
- Ability to send logs in real-time to any additional external reporting systems such as SIEMs, including Splunk
- Infinite scale and storage in the cloud eliminating large database appliances and providing a roadmap to future growth

Traditional Reporting Challenges

The volume of Internet traffic is increasing exponentially. The need to understand user behavior starts with the ability to capture and associate log events to each Internet access attempted by users and devices. The volume of logging is increasing exponentially creating strain for reporting systems to keep up with the load. To make things worse, HTTPS encryption is masking user activity leaving administrators blind to what is really going on within the organization. Some of the typical challenges faced when attempting to gain an understanding of Internet use within an organization include:

- The inability to determine which user created which access due to the lack of usernames within log reports
- Even when username association is possible, traditional Internet security solutions may require prompting users to get credentials and association does not occur automatically
- No visibility into encrypted HTTPS traffic creating massive blind spots with HTTPS traffic headed towards accounting for 80% of all network traffic
- Reporting that contains only domain names instead of full URLs which makes it difficult to understand the actual user behavior, especially on sites like Google where search terms are important
- Challenges getting reporting for users that go mobile and are no longer within the physical network perimeter
- Too much noise in the logs making it difficult to determine what is actually occurring on the Internet
- Lack of interactive drill down reports needed for investigations
- Slow report generation due to the large volume of logs within the reporting databases
- Very little reporting information due to missing log events or reduced log events which some platforms use to reduce load within the reporting database
- The need to manually backup logs that need to be held for compliance including the need to purchase and maintain backup log servers
- Difficulty in pinpointing high risk users and high risk user activity

Solve Traditional Reporting Challenges With iboss cloud



The iboss cloud was designed with the modern Internet in mind and includes the most comprehensive reporting needed to reduce risk, increase user productivity and provide the insight administrators demand.

Usernames Automatically Associated With Internet Activity

The iboss cloud automatically associates usernames with log and reporting activity which provides the necessary information to re-mediate issues quickly. Usernames are automatically obtained transparently to the user for a seamless end user experience. Usernames are included in logs and drill down reports.

Full URL Details for Internet Activity

The need to obtain the full URL being accessed is critical to understand Internet activity with context. For example, while some reporting platforms include just the base domain of a website, such as "google.com", the iboss cloud will include the full URL such as "google.com/shopping". Some Internet security platforms do not have access to full URL details due to the type of technology being used to secure Internet access or due to the inability to drill into encrypted HTTPS traffic. The iboss cloud automatically obtains full details into every access to provide full details within log reports.

Detailed Log Reports for Mobile Users

Mobility is the future, as cloud SaaS applications continue to transform the way people work. The iboss cloud runs in the cloud where the applications run, which means that users are always connected to Internet security at all times. This means that the iboss cloud will also capture and store detailed log and reporting events even when users are mobile while they work on devices owned by the organization. This ensures risky sites and behaviors are kept off of organization devices which lead to infection and can compromise other devices when they return back to the organization. Use iboss cloud to solve organization mobile and cloud initiatives while maintaining control and visibility while users are remote.

Logs With All of the Details Necessary to Identify and Re-mediate Issues

The iboss cloud will log reporting events with detailed information including username, user group, source IP Address, destination IP Address, full URL, categories, resulting action and more. These details can be used to back-trace an issue and generate highly detailed reports for administrators and executive staff.

Anonymize Logging and Reporting

In cases where some of these logging fields must be anonymized, the iboss cloud can encrypt fields such as username, source IP and group which can only be unlocked by administrators with privileges to do so. This allows the ability to provide access to logs and reports to administrators without exposing PII or violating compliance.

Detailed Interactive Drill Down Reports

The iboss cloud will automatically generate interactive drill down reports that can be used for investigations. This compiles information into easy to read dashboards that an administrator can use to drill down into the specific details of an incident. The reports include aggregate information such as top users, web sites, top categories, infected devices, risky users and more.

Real-time Dashboards That Can Be Used to Identify and Resolve Issues Quickly

The real-time dashboards in iboss cloud provide a real-time view of what is happening on the network now. If something changes on the network causing issues or slowdown, the iboss cloud can be used to pinpoint exactly what the issue is. The real-time dashboards also include connection level details including packet and byte counts. Top users by bandwidth are also included to understand problematic behavior quickly.

Real-Time Alerts For High Risk Searches and Behavior

The iboss cloud can be configured to alert administrators whenever a high risk search or behavior occurs. The alerts can be configured to be sent to different administrators depending on the user or group from which that behavior occurred to get the information to the right place at the right time. Alerts include high risk search engine searches, including search keywords, to prevent high risk behavior from compromising a device or putting the institution at risk due to compliance violations.

Send Logs to Any External SIEM in Real-Time

The iboss cloud can send any reporting logs it stores to any additional external SIEM in real-time. This enriches the data available to the SIEM by providing insight into user Internet activity regardless of user location. In addition, the sending of logs does not require any external forwarders and can send logs to multiple SIEMs concurrently. Built-in connectors for Splunk are included and standard connector options that leverage syslog and SFTP can be used to connect any external SIEM.

Infinite Reporting Storage in the Cloud

The iboss cloud processes and stores reporting data in the cloud. This means that any amount of data can be stored without worrying about larger and more expensive reporting appliances as bandwidth exponentially increases. For organizations that need reporting data on-site, private cloud can store reporting data within the organization's datacenter or behind the organization's firewall.

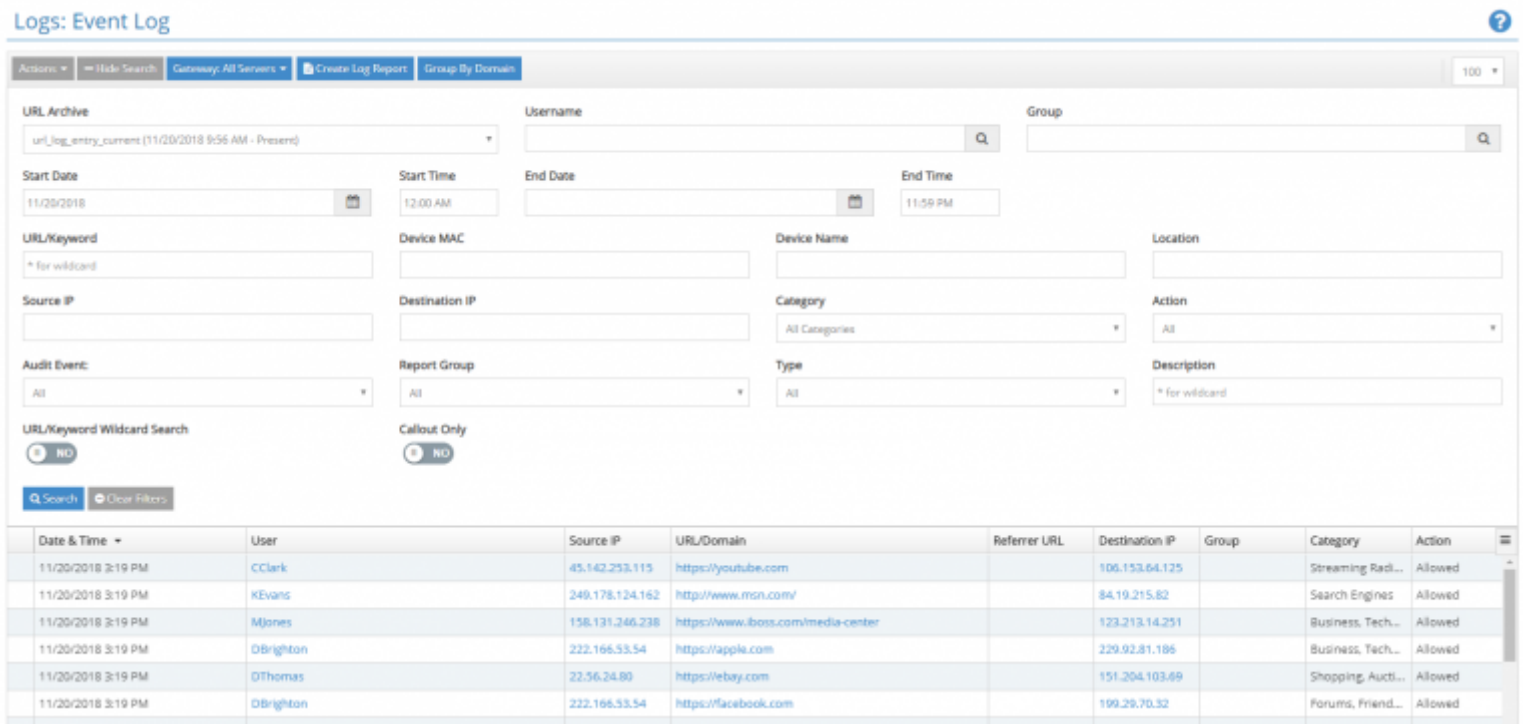
How It Works

Reporting is automatically enabled with every iboss cloud subscription:

1. Get an active iboss cloud account
2. Connect users to iboss cloud using an iboss cloud connector. Connectors are available for virtually all Operating Systems including Windows, Mac, iOS and Chromebooks
3. As users access the Internet, activity is automatically logged and associated to the user automatically. Drill down reports are automatically generated

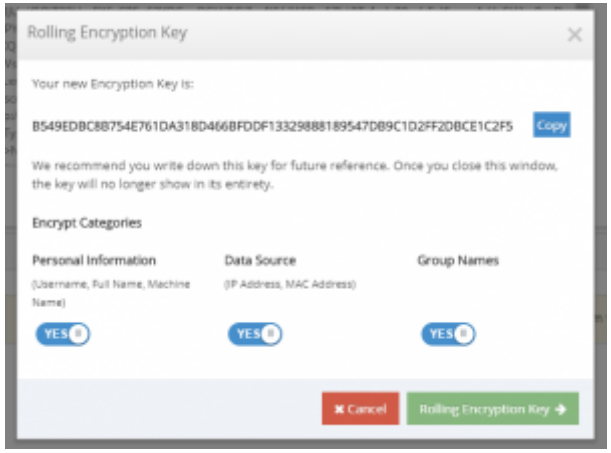
Feature Highlights

Detailed Log Events Including Username



The iboss cloud log events include usernames and all information needed to associate logs. In addition, very granular filters are provided to search log events down to the minute. Reports for users can be generated and emailed to requesting administrators in the background for maximum efficiency.

Log Anonymization



Anonymize user information so that reporting can be granted to delegated administrators without comprising sensitive user identity. Administrators with privileges will have the ability to unlock the username when necessary.

Real-time Reporting Dashboards

The advanced reporting dashboards provide visualization tools to identify issues quickly. The dashboards are interactive and administrators can drill into the data to get the information necessary to resolve issues quickly.

Pricing

Advanced Reporting Capabilities	
Advanced granular reporting capabilities are included at no cost with every iboss cloud subscription	Contact Us

For more information on iboss cloud reporting, please visit https://www.iboss.com/platform/detailed-logging-and-reporting.

About iboss

iboss is a cloud security company that provides organizations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, iboss is designed to make transitioning from security appliances to cloud security a seamless process. iboss is trusted by more than 4000 organizations worldwide, spans over 100 points of presence globally and is backed by over 110 patents.

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