iboss™
NETWORK SECURITY

Product Brochure

iboss SWG Web Security Solution

- HTTP/S Filter
- Application Management
- Mobile / BYOD Security
- Bandwidth/QoS
- Threat & Event Console

www.iboss.com

Phantom Technologies, Inc. DBA iboss SWG Web Security (P) 877.742.6832 Sales@iboss.com U.S. HQ 9950 Summers Ridge Rd., Bldg. 160 San Diego, CA 92121

The iboss SWG Suite

Choose an all-in-one solution, or customize the suite to your network's needs.

- Web Filter
- Malware/DLP/Threat
- Next-Generation Firewall
- Threat & Event Console
- MDM & EMM
- Mobile Security
- Email Spam Boss
- Email Archiver

About iboss Network Security, a division of Phantom Technologies, Inc.

Founded in 2003, Phantom Technologies, Inc. is a global provider of network security solutions. Its iboss Network Security line of products deliver network traffic insight and threat mitigation. Proprietary engineering powerfully secures high-demand networks for web content management, intrusion, mobile device security and management, and email security.

To learn more about our services:
www.iboss.com

Main: 1-877-742-6832 ext. 1
Support: 1-858-568-7051 ext. 3

iboss Network Security is recognized by Gartner, the world's leading information technology research and advisory company. In addition to Gartner, iboss has received numerous awards related to web filtering and Internet security.

Gartner®

SC MAGAZINE

OVERALL RATING	★★★★★
Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for Money	★★★★★

iboss Network Security

Web filtering has become an increasingly complex issue as people everywhere have come to rely on the Internet and use it for their daily work. However, challenges surface when instead of using the Internet for work-appropriate activities, professionals are viewing inappropriate material and/or violating compliance regulations set forth by CIPA, HIPPA and Acceptable Use Policy (AUP) requirements. Without the support of truly effective filtering, such violations and misuses pose major network problems for organizations and professionals of all types, but some industries, including health care and education, are particularly vulnerable. Whether it's nurses, doctors, teachers, students, employers and their employees, all can experience a host of security breakdowns and breaches without foolproof filtering. Whether devices are organization-owned or brought from home, this security is crucial for both wired and wireless devices.

Most filtering solutions on the market provide an "all or nothing" approach, which hinders productivity. These come with "limited" policies, which block access to those who need it most and give too much access to those who require restrictions. This formula not only creates a lot of device login hurdles and headaches, but it also contributes to overall user frustration, which leads to negativity, even low workplace morale. (No one likes technological inefficiencies, right?)

As if that's not enough, most filtering solutions have limited or very complicated reporting that makes it tough to spot problems easily on the network. Detection is difficult whether it relates to someone who is using too much bandwidth and interrupting mission critical traffic, someone causing viruses on the network due to poor Internet habits, or someone posing security threats that could lead to lawsuits and costly technology interruptions.

The iboss SWG Web Security Solution is a comprehensive yet user-friendly solution that scans across SSL/HTTPS to protect sensitive information, controls network resources through bandwidth management features, regulates the way social media content is accessed, identifies threats, and reports traffic. In addition, it allows for ultimate control and flexibility, thanks to advanced filtering policies tha can be set according to user group(s).

Bottom line: The iboss SWG Web Security Solution is a cost-effective, must-have solution that addresses the explosive complexities of today's filtering and network security challenges.

iboss SWG Web Security Solution

Features

Web Filtering

- HTTP/S Web filtering.
- Scan across SSL to identify embedded threats.
- Social media management.
- Flexible URL vs. domain controls.
- Secure across all 65,535 ports, including all protocols.

Application Control

- Layer 7 DPI, Signature, and Heuristics provide advanced detection of SSL-based applications and proxy avoidance tools.
- Control chat, P2P, torrents, FTP transfers, gaming, and more.
- Identify and protect against internal servers, rouge-encrypted connections, and proxy avoidance applications.

Threat & Event Console

- Instant access to archived network activity logs.
- Live threat dashboards provide iboss exclusive threat GeoMapping, DLP, and directory integration.
- Ad-Hoc reporting and automated report scheduling.
- Delegate access of reports for local insight on network activity.
- Dynamic bandwidth plotter with instant heat maps, tracking bandwidth consumption by connection, packets and data usage.

Bandwidth Management

- Dynamically control bandwidth during peak hours, ensuring network-critical applications are prioritized while recreational traffic is reduced.
- Unique ability to bind to network directories and apply polices to groups, users, or subnets.
- Apply policies using predefined categories, IP/TCP, and domain-to-target "network specific" issues.

BYOD and Mobile Security

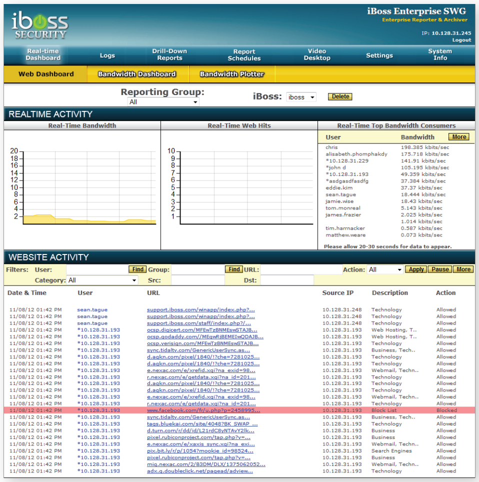
- High risk quarantine.
- On/off premise security.
- Bandwidth QoS/Throttling.

Unmatched Performance
Designed for High-Demand Networks

Ensures Regulatory Compliance: CIPA and HIPPA

Issue: Nowadays, it has become increasingly tough to manage the network by filtering URLs. With the emergence of Web 2.0 and HTTPS, as well as the growing incorporation of mobile devices and BYOD in daily operations, it's become imperative to secure the network beyond wired devices. In addition, generic reporting of URL access fails to provide complete insight on the network resources utilized, and it lacks the ability to pinpoint the latest threats.

Solution: To address the "new Web," the iboss SWG Web Security Solution secures all aspects of Internet traffic including web filtering, SSL access, applications, bandwidth throttling/QoS, on/off-premise mobile security, and BYOD management tools. This comprehensive security suite is tailored to secure all aspects of wired and wireless traffic, both on and off-premise. Where traditional web filters address web access in a "good/bad" approach, iboss SWG Web Security focus on securing technology in the organization even if users are accessing the network through a traditional PC or BYOD, or from an off-premise locale.



User	Bandwidth
chris	198.385 kbits/sec
alisabeth.phomphakdy	175.718 kbits/sec
*10.128.31.229	141.91 kbits/sec
*john d	105.195 kbits/sec
*10.128.31.193	49.359 kbits/sec
*asdgasdfasdfg	37.384 kbits/sec
eddie.kim	37.37 kbits/sec
sean.tague	18.444 kbits/sec
jamie.wise	18.43 kbits/sec
tom.monreal	5.143 kbits/sec
james.frazier	2.025 kbits/sec
	1.014 kbits/sec
tim.harrnacker	0.587 kbits/sec
matthew.weare	0.073 kbits/sec

Please allow 20-30 seconds for data to appear.

Date & Time	User	URL	Source IP	Description	Action
11/08/12 01:42 PM	sean.tague	support.iboss.com/winapp/index.php?...	10.128.31.248	Technology	Allowed
11/08/12 01:42 PM	sean.tague	support.iboss.com/winapp/index.php?...	10.128.31.248	Technology	Allowed
11/08/12 01:42 PM	sean.tague	support.iboss.com/staff/index.php?/...	10.128.31.248	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	ocsp.digicert.com/MFEwTzBNMEswSTAJB...	10.128.31.193	Web Hosting, T..	Allowed
11/08/12 01:42 PM	*10.128.31.193	ocsp.godaddy.com//MEgwRjBEMEIwQDAJB...	10.128.31.193	Web Hosting, T..	Allowed
11/08/12 01:42 PM	*10.128.31.193	ocsp.verisign.com/MFEwTzBNMEswSTAJB...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	sync.tidaltv.com/GenericUserSync.as...	10.128.31.193	Business, Tech..	Allowed
11/08/12 01:42 PM	*10.128.31.193	d.agkn.com/pixel/1840/!?che=7281025...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	d.agkn.com/pixel/1840/!?che=7281025...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	e.nexac.com/e/xrefid.xgi?na_exid=98...	10.128.31.193	Webmail, Techn..	Allowed
11/08/12 01:42 PM	*10.128.31.193	r.nexac.com/e/getdata.xgi?na_id=201...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	d.agkn.com/pixel/1840/!?che=7281025...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	d.agkn.com/pixel/1840/!?che=7281025...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	e.nexac.com/e/xrefid.xgi?na_exid=98...	10.128.31.193	Webmail, Techn..	Allowed
11/08/12 01:42 PM	*10.128.31.193	r.nexac.com/e/getdata.xgi?na_id=201...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	www.facebook.com/fr/u.php?p=2458995...	10.128.31.193	Block List	Blocked
11/08/12 01:42 PM	*10.128.31.193	sync.tidaltv.com/GenericUserSync.as...	10.128.31.193	Business, Tech..	Allowed
11/08/12 01:42 PM	*10.128.31.193	tags.bluekai.com/site/4048?BK_SWAP_...	10.128.31.193	Technology	Allowed
11/08/12 01:42 PM	*10.128.31.193	d.turn.com/r/dd/id/L21rdC8yNTAvY2lk...	10.128.31.193	Business	Allowed
11/08/12 01:42 PM	*10.128.31.193	pixel.rubiconproject.com/tap.php?v=...	10.128.31.193	Business	Allowed
11/08/12 01:42 PM	*10.128.31.193	e.nexac.com/e/xaxis_sync.xgi?na_exi...	10.128.31.193	Webmail, Techn..	Allowed
11/08/12 01:42 PM	*10.128.31.193	pix.bit.ly/r/p/1054?mookie_id=98524...	10.128.31.193	Search Engines	Allowed
11/08/12 01:42 PM	*10.128.31.193	pixel.rubiconproject.com/tap.php?v=...	10.128.31.193	Business	Allowed
11/08/12 01:42 PM	*10.128.31.193	mig.nexac.com/2/B3DM/DLX/1375062052...	10.128.31.193	Webmail, Techn..	Allowed
11/08/12 01:42 PM	*10.128.31.193	adx.g.doubleclick.net/pagead/adview...	10.128.31.193	Technology	Allowed

iboss SWG Web Security Combines:

- Web Filtering (HTTP/S)
- Scan Inside SSL
- Layer 7 Application Management DPI/Heuristics/Signatures
- BYOD Management- Authentication, Bandwidth, High Risk Quarantine
- Mobile Security - On/Off Premise Security
- Bandwidth Throttling and QoS
- Integrated SWG Threat & Event Console
- Single Pane of Glass Reporting for On/Off Premise Devices

Application, HTTPS, Web 2.0

Web 2.0 introduced the need to protect traffic outside standard Port 80 and 443. New applications such as torrents, annonymizers, and chat applications such as Yahoo and Google Chat must use nonstandard ports for communication. Securing these ports ensures network compliance and reduces threat exposure while enforcing the organization's acceptable use policies (AUP).

Solution Highlights

Scanning Across SSL/HTTPS

SSL is essential to protect sensitive information on financial sites and other types of online locales, but it's also being used for social media platforms like Facebook and YouTube. Utilizing advanced techniques, iboss SWG Web Security dynamically identifies all traffic, including SSL, with the help of advanced algorithms and signatures that lack cumbersome configurations.

REAL-TIME BANDWIDTH MAP - TOP DESTINATIONS BY BANDWIDTH
Map
Satellite
Greenland
Iceland
Finland
Sweden
Norway
Russia
Canada
United Kingdom
Poland
Germany
Ukraine
France
Kazakhstan
Mongolia
Spain
Italy
Turkey
China
South Korea
Japan
United States
North Atlantic Ocean
North Pacific Ocean
Iraq
Iran
Afghanistan
Pakistan
Algeria
Libya
Egypt
Saudi Arabia
India
Mexico
Mali
Niger
Chad
Sudan
Thailand
Nigeria
Ethiopia
Venezuela
Colombia
Kenya
DR Congo
Tanzania
Indonesia
Papua New Guinea
Peru
Brazil
Bolivia
Angola
Namibia
Botswana
Madagascar
Indian Ocean
South Pacific Ocean
Chile
South Atlantic Ocean
South Africa
Australia
Argentina
New Zealand
Google
Map data ©2012 MapLink, Tele Atlas - Terms of Use

Protect Network Resources/Bandwidth QoS

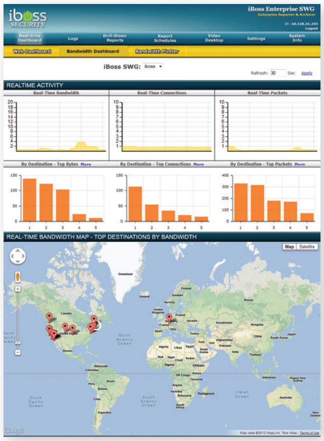
iboss Bandwidth Management delivers control and visibility of network traffic. Flexible policies can be applied to throttle non-critical traffic during peak hours while ensuring that network-critical access is retained. With its real-time bandwidth logs and comprehensive data reports, IT can identify the area of bandwidth usage. Advanced controls allow policies to be set by predefined categories, domain, IP, or TCP/UDP and then applied to different groups. Management is refreshingly seamless and simple.

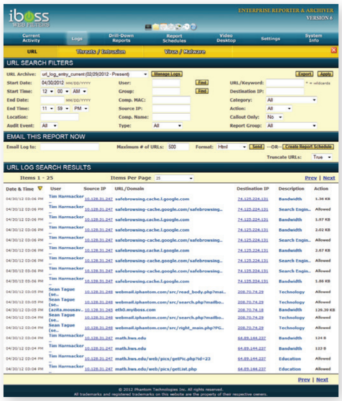
Social Media Content Management

Expansive social media management options provide "clean" access to YouTube, Google Management Suite and both their services. They also offer Google Clean Image Search and page-content control for social media sites. Powerful YouTube content management enables organizations to strip comments, ads, and unrelated videos dynamically and directly from YouTube search results.

Identify Threats & Report Traffic

iboss SWG Web Security contains the powerful iboss SWG Enterprise Forensic Reporter to provide best-of-breed network reporting, forensic search abilities, and drill-down detail of all network traffic. iboss SWG Forensic Reporter provides dynamic real-time threat dashboards to pinpoint threats, bandwidth usage, and user activity. It also includes the Bandwidth Plotter, so administrators can track bandwidth consumption through a bandwidth plotter and heat map charts, plus search functions to track individual connections. The proprietary Global Geotagging Map over IP provides live, visual insight on wherever network traffic is originating from, across the globe.





URL SEARCH FILTERS

URL Archive: url_log_entry_current (02/29/2012 - Present)
Start Date: 04/30/2012 MM/DD/YYYY
Start Time: 12 00 AM
End Date: MM/DD/YYYY
End Time: 11 59 PM
Location:
Audit Event: All
User:
Group:
Comp. MAC:
Source IP:
Comp. Name:
Type: All
URL/Keyword: * = wildcards
Destination IP:
Category: All
Action: All
Callout Only: No
Report Group: All

EMAIL THIS REPORT NOW

Email Log to:
Maximum # of URLs: 500
Format: Html
--OR--
Truncate URLs: True

URL LOG SEARCH RESULTS

Items 1 - 25 Items Per Page 25 Prev | Next

Date & Time	User	Source IP	URL/Domain	Destination IP	Description	Action
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing.cache.l.google.com	74.125.224.131	Bandwidth	1.36 KB
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing-cache.google.com/safebrowsing..	74.125.224.131	Search Engin..	Allowed
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing.cache.l.google.com	74.125.224.131	Bandwidth	1.97 KB
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing.cache.l.google.com	74.125.224.131	Bandwidth	2.02 KB
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing-cache.google.com/safebrowsing..	74.125.224.131	Search Engin..	Allowed
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing.cache.l.google.com	74.125.224.131	Bandwidth	2.67 KB
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing-cache.google.com/safebrowsing..	74.125.224.131	Search Engin..	Allowed
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing-cache.google.com/safebrowsing..	74.125.224.131	Search Engin..	Allowed
04/30/12 03:06 PM	Tim Harrnacker	10.128.31.247	safebrowsing.cache.l.google.com	74.125.224.131	Bandwidth	1.86 KB
04/30/12 03:05 PM	Sean Tague (se..	10.128.31.248	webmail.iphantom.com/src/read_body.php?mai..	208.70.74.29	Technology	Allowed
04/30/12 03:05 PM	Sean Tague (se..	10.128.31.248	webmail.iphantom.com/src/search.php?mailbo..	208.70.74.29	Technology	Allowed
04/30/12 03:05 PM	(azita.mousav..	10.128.31.245	eth0.myiboss.com	208.70.74.18	Bandwidth	120.30 KB
04/30/12 03:04 PM	Sean Tague (se..	10.128.31.248	webmail.iphantom.com/src/search.php?mailbo..	208.70.74.29	Technology	Allowed
04/30/12 03:04 PM	Sean Tague (se..	10.128.31.248	webmail.iphantom.com/src/right_main.php?PG..	208.70.74.29	Technology	Allowed
04/30/12 03:04 PM	Tim Harrnacker	10.128.31.247	math.hws.edu	64.89.144.237	Bandwidth	124 B
04/30/12 03:04 PM	Tim Harrnacker	10.128.31.247	math.hws.edu	64.89.144.237	Bandwidth	123 B
04/30/12 03:04 PM	Tim Harrnacker	10.128.31.247	math.hws.edu/web/pics/getPic.php?id=23	64.89.144.237	Education	Allowed
04/30/12 03:04 PM	Tim Harrnacker	10.128.31.247	math.hws.edu/web/pics/getList.php	64.89.144.237	Education	Allowed

Prev | Next

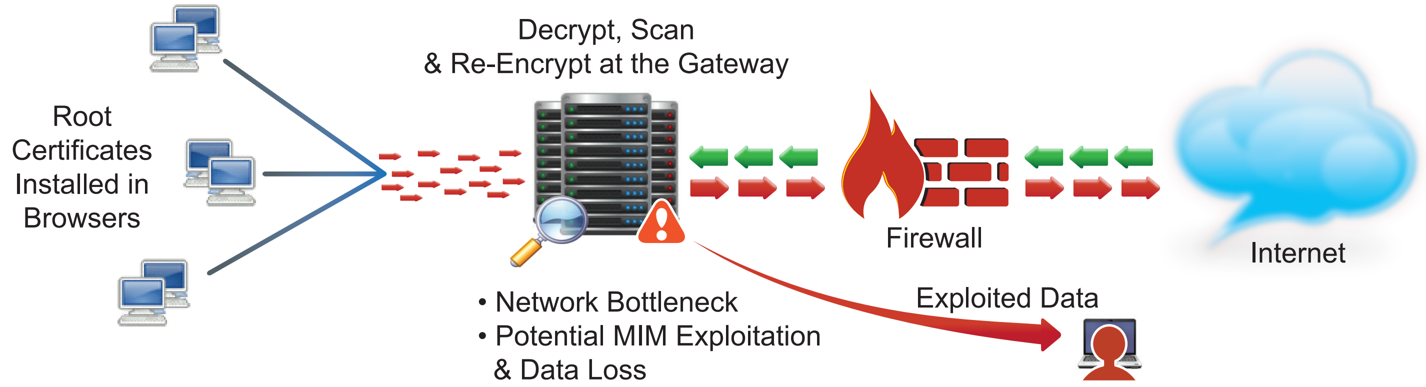
© 2012 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

Scanning Across HTTPS/SSL Traffic

The Web has become an essential aspect of daily operations with enterprises everywhere. Countless organizations rely on this must-have solution for everything from web surfing for research to tapping specific, browser-based applications (e.g., Google Apps, CRM tools and social media) for marketing purposes. Due to their sensitive nature, many of these resources are encrypted through HTTPS to secure the data. This encryption creates a “blind spot” for organizations seeking to manage network traffic. Unfortunately, hackers, annonymizers, and other threats use this blind spot to exploit network resources under the encryption umbrella.

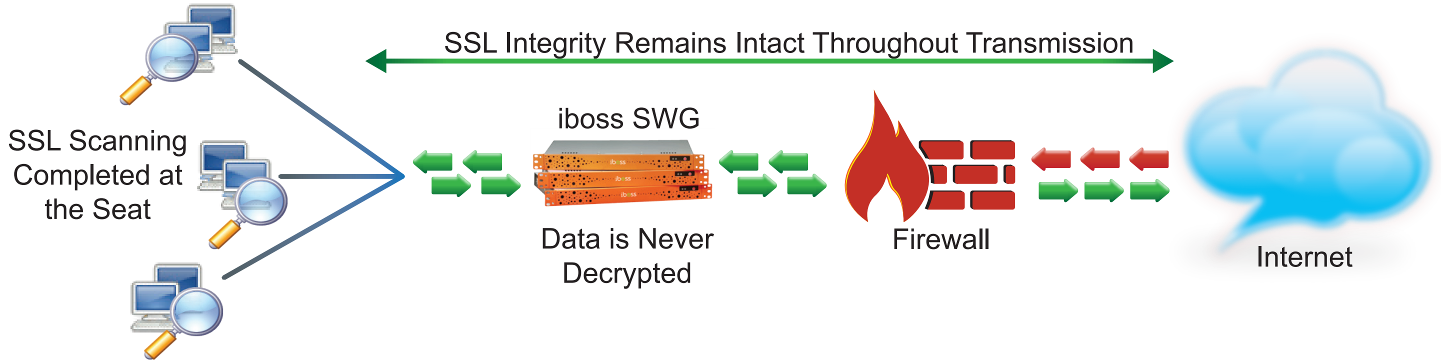
Issues With Typical SSL Scanning – Root Certificates

Typically, solutions utilize root certificates to scan HTTPS traffic. This creates a network bottle neck on the network where the traffic is decrypted at the gateway. Additionally, this leaves networks vulnerable to “man-in-the-middle” attacks.


Root Certificates Installed in Browsers
Decrypt, Scan & Re-Encrypt at the Gateway
Firewall
Internet
• Network Bottleneck
• Potential MIM Exploitation & Data Loss
Exploited Data

The iboss Difference – Uncompromised Security and Unmatched SSL Performance

iboss SWG Web Security provides advanced EdgeScan HTTPS scanning at the individual workstations vs. at the network gateway. Edgescan ensures that traffic flows uninterrupted from the workstation to its final destination and prevents network bottlenecks. In addition, this proprietary technology prevents “man-in-the-middle” attacks. Traffic is never modified once it leaves the workstation, so all data remains intact. The EdgeScan technology protects networks against threats embedded within HTTPS while maintaining data integrity and network performance.


SSL Integrity Remains Intact Throughout Transmission
SSL Scanning Completed at the Seat
iboss SWG
Data is Never Decrypted
Firewall
Internet

BYOD Management Suite

Bring Your Own Device/Technology (BYOD/T) is one of the fastest moving sectors of technology. BYOD allows organizations to increase technology and productivity without boosting budgets. However, with the benefits of BYOD also come concerns and pain points.

iboss SWG Web Security's integrated BYOD Management suite provides network administrators the tools to ensure that BYOD access is filtered from malware, botnets, and DLP. It also preserves bandwidth on the BYOD network, supporting and upholding the integrity of mission-critical traffic. To properly identify BYOD users not using network access control (NAC), iboss SWG Web Security provides a captive portal that automatically binds to a network directory or LDAP. It then applies the directory-group-based policies, allowing users consistent web access whether they're on a wired or wireless device. Advanced application controls and the iboss High Risk Auto Quarantine automatically lock user devices when high-risk activities, such as illegal file downloading or annonymizer use, are detected. The BYOD Management suite is included in all iboss SWG Web Security Solutions to secure the wired and wireless networks.

iboss SWG Web Security BYOD Benefits:

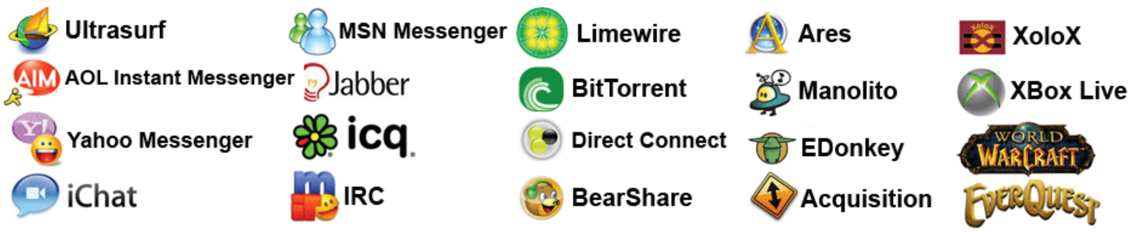
- Extend compliance and AUP to BYOD devices.
- Scan and filter known and unknown threats including Malware, Botnets, and DLP.
- BYOD bandwidth throttling and QoS to ensure mission critical traffic remains uninterrupted.
- BYOD directory integration and binding across Active Directory, eDirectory, Open Directory, and LDAP.
- High Risk User Auto Quarantine – automatically locks users attempting to conduct illegal activity such as music and file downloading.

Application Firewall – Securing the Network Beyond Port 80 and 443

Application Management

Today, many applications use proprietary signatures and ports to communicate properly. Some of these applications, such as Skype and WebEx, are required for the organization to operate while other applications may introduce threats. Simple content management through Port 80 or 443 does not provide the security or flexibility needed to secure the gateway.

To effectively manage all traffic at the gateway while securing against unwanted applications, iboss Application Scanning easily monitors traffic across all 65,535 ports including UDP protocol, by combining layer 7 inspection and deep-packet inspection (DPI), plus all of the necessary signatures and heuristics.

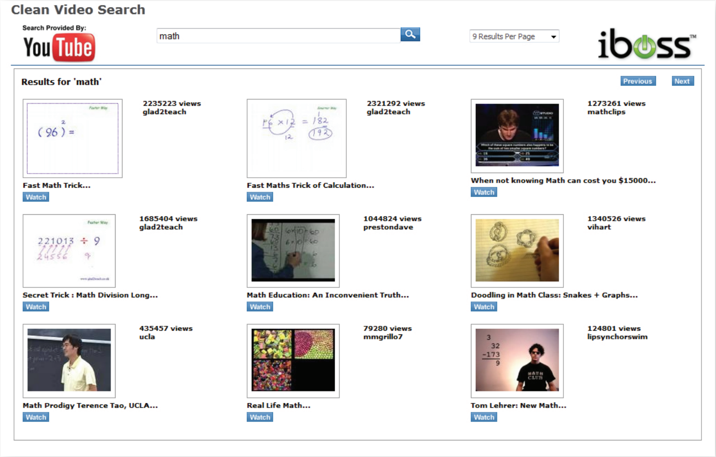


Malware and Botnet Security

By blending best-of-breed Bitdefender's malware signatures and heuristic database with Phantom Technologies' database at the gateway, organizations can achieve a layered security approach to an already existing structure. Packets are scanned at the gateway, utilizing zero-day signatures that eliminate potential threats from the traffic flowing to workstations and protect network resources from exposure to new threats.

YouTube Management

YouTube has become very popular with countless organizations and provides many resources for internal and research purposes. iboss SWG Web Security offers a comprehensive suite of options to manage this access. It's designed to both prevent unwanted activity by select users and preserve network resources. These advanced YouTube management controls maintain the correct level of access based on an organization's needs.



Clean Video Search

Search Provided By: YouTube

math

9 Results Per Page

Results for 'math'

2235223 views glad2teach — Fast Math Trick...

2321292 views glad2teach — Fast Maths Trick of Calculation...

1273261 views mathclips — When not knowing Math can cost you $15000...

1685404 views glad2teach — Secret Trick : Math Division Long...

1044824 views prestondave — Math Education: An Inconvenient Truth...

1340526 views vihart — Doodling in Math Class: Snakes + Graphs...

435457 views ucla — Math Prodigy Terence Tao, UCLA...

79280 views mmgrillo7 — Real Life Math...

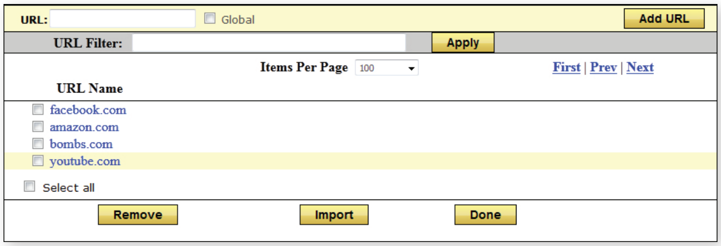
124801 views lipsynchorswim — Tom Lehrer: New Math...

Clean YouTube Content Management

Powerful YouTube content management enables organizations to strip comments, ads, and unrelated videos dynamically and directly from YouTube search results. This blocks inappropriate comments and unwanted material.

HTTPS YouTube Management

Thanks to advanced algorithms and signatures, administrators can quickly and effectively block SSL access to YouTube without affecting Google Docs or other Google services. No advanced configuration is required.



URL: □ Global

URL Filter:

Items Per Page 100

URL Name

□ facebook.com
□ amazon.com
□ bombs.com
□ youtube.com

□ Select all

Expanded Security for Google Services

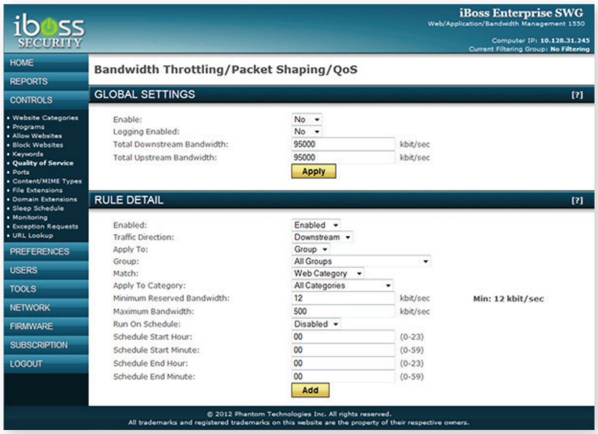
iboss Clean Image and Translation Filtering

Google is a growing part of the daily operations for many organizations. Services such as Google Images and Translation provide needed access for research and productivity. Due to the caching of these services by Google, organizations are now forced to rely on Google Safe Search to enforce the AUP. This often proves difficult, however, and forces organizations to remove access to these services. Thanks to features such as Clean Image Search and Translation Filtering, iboss Web Filter provides expanded security for Google services like Images and Translation. This is achieved by iboss scanning content and applying the authenticated user's specific-access policy against the search results and then stripping restricted content directly from the search results.

— something safe search misses!

Quality of Service / Bandwidth Management

iboss Bandwidth Management delivers control and visibility of network traffic. Flexible policies can be applied to throttle non-critical traffic during peak hours while ensuring network-critical access is retained. With real-time bandwidth logs and comprehensive data reports, IT can identify areas of bandwidth usage. Advanced controls allow policies to be set by predefined categories, domain, IP, or TCP/UDP, and then applied to different groups. This provides seamless, simple management.



iBoss Enterprise SWG
Web/Application/Bandwidth Management 1550

Computer IP: **10.128.31.245**
Current Filtering Group: **No Filtering**

Bandwidth Throttling/Packet Shaping/QoS

GLOBAL SETTINGS

Enable:	No	
Logging Enabled:	No	
Total Downstream Bandwidth:	95000	kbit/sec
Total Upstream Bandwidth:	95000	kbit/sec

RULE DETAIL

Enabled:	Enabled		
Traffic Direction:	Downstream		
Apply To:	Group		
Group:	All Groups		
Match:	Web Category		
Apply To Category:	All Categories		
Minimum Reserved Bandwidth:	12	kbit/sec	**Min: 12 kbit/sec**
Maximum Bandwidth:	500	kbit/sec	
Run On Schedule:	Disabled		
Schedule Start Hour:	00	(0-23)	
Schedule Start Minute:	00	(0-59)	
Schedule End Hour:	00	(0-23)	
Schedule End Minute:	00	(0-59)	

© 2012 Phantom Technologies Inc. All rights reserved.
All trademarks and registered trademarks on this website are the property of their respective owners.

DMCR (Desktop Monitor Control Record)

Monitor, Control & Record Desktops

To expand security and identify compliance and AUP concerns, organizations cannot rely solely on web logs. To provide more comprehensive insight on violations, the iboss SWG Web Security Solution provides automated desktop recording on violations. Administrators simply set violation triggers, and DMCR will automatically record the live user desktop and then transfer and store recordings for up to one year.

In addition, at any given time, administrators can view, control, or record up to 10 desktops per every one monitor. This provides a direct line of site for any potential violation concerns or simply improves support across the organization.

The DMCR feature is an exclusive feature to iboss SWG Web Security Solutions and delivers unmatched, "outside the box" insight to qualify events more accurately.

Protection Against Proxies

A Layered Defense Against Proxy Circumvention

Proxies pose a risk to networks by introducing web access that potentially violates the AUP as well as makes the network susceptible to threats, including viruses, botnets, malware, etc. To secure the network fully against proxies and proxy applications such as Ultrasurf and Hotspot shield, iboss SWG Web Security secures traffic in a layered approach.

Designed for Fiber

10Gbs Wire Speed Performance at Layer 7

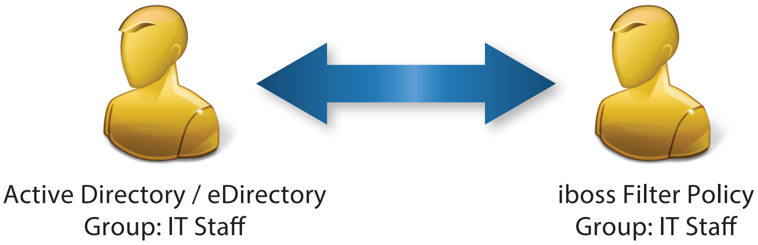
iboss SWG Web Security is based upon proprietary engineering. Designed for fiber networks, the iboss SWG Web Security Solution's architecture is scalable and capable of over 6 million concurrent TCP/IP connections, 250,000 devices, and10Gbps throughput of filtered traffic on a single appliance.

With multi-threading technology, proprietary algorithms, intelligent database management, and EdgeScan HTTPS processing, iboss SWG Web Security is engineered to scale with your network without introducing latency, reducing the total cost of ownership (TCO).

Directory and Management

Single Sign-on Transparent Policy

Users can be transparently assigned to an iboss group as soon as they log onto their workstation. This process is based on their group membership in the Active Directory or eDirectory. Active Directory/eDirectory Groups are matched to the iboss filtering group in a one-to-one fashion.



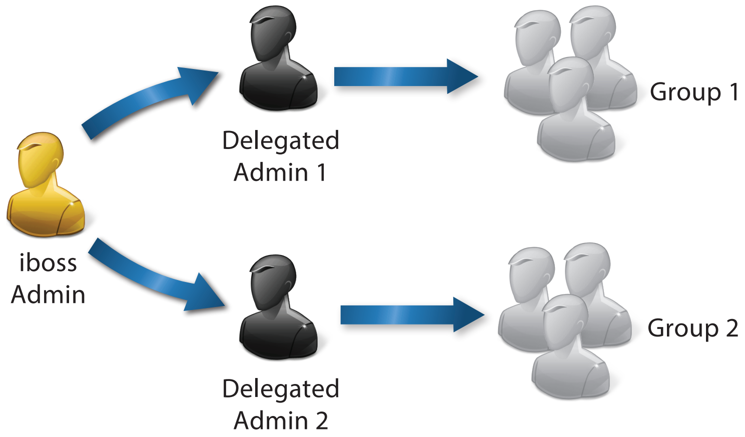
Seamless, Client-Free Integration

With no agents, thin clients, or browser settings required at the workstation, directory authentication is quick and easy. Flexible options include directory plugins or the use of log on/log off scripts. Users authenticate once when accessing the workstation, and then iboss gathers the user name, IP, group membership, and netbios name. Then it applies the policy based on group membership.

Administration

Delegated Administrators

The iboss SWG Web Security Solution allows you to create multiple Sub-Administrators (delegated administrators) to log into the iboss interface and manage filtering rules for specific filtering groups. This allows for separate iboss administrators to manage the rules for a specific group, department, class, etc., without having access to other filtering groups or rules.



Features

Live Threat & Bandwidth Dashboards

- Live threat dashboards provide iboss-exclusive threat GeoMapping, DLP, & Directory Integration.
- Live bandwidth dashboard and plotter enables advanced bandwidth tracking with comprehensive controls.

Bandwidth Heat Map

- Delivers a dynamic bandwidth plotter with instant heat-map tracking for detecting bandwidth consumption by connection, packets and data usage.

URL/Ad-Hoc Reports

- Instant URL logs and ad-hoc reports on all websites visited, recording date, time, user, URL, and many more discoveries, while also requesting quick information on network activity.

Dynamic Drilling

- Allows access to any and all events, providing a dynamic drill-down interface that reveals the user.

Site Callouts

- Delivers clear insight on user activity by dynamically removing unwanted website "chatter."

Automated Report Scheduling

- Compliance-ready reports are automated and distributed on need-based schedules.

Automated Backups

- Carves out more time to focus on network priorities and ensures that compliance-required data is consistently and securely archived.

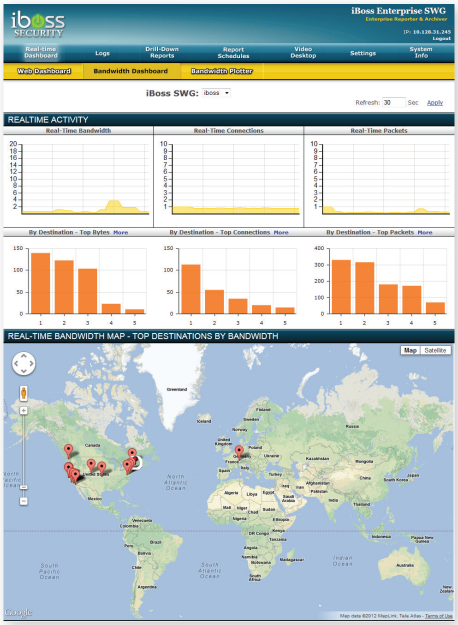
Distributed Enterprise

- Centrally view network activity logs and identify enterprises and mobile devices.

Integrated iboss SWG Threat & Event Console

Introduction

The iboss SWG Threat & Event Console changes how we approach user-activity reporting and threat mitigation by addressing with whom and where our network is communicating. By tapping exclusive features such as threat GeoMapping and heat map technology to identify threats lurking in the background, iboss Threat & Event Console provides a new approach to network activity monitoring. iboss SWG Threat & Event Console also includes a consolidated dashboard of the iboss SWG product line in one view. Within seconds, administrators gain a 360-degree view of each network user, including Web, application, bandwidth, packet consumption, data loss, email malware, and threat activity. This consolidates compliance reporting, increases network insight, and reduces the total cost of ownership (TCO).



iBoss SWG: iboss

Refresh: 30 Sec

iboss SWG Threat & Event Console Benefits:

- Consolidated Version of All iboss SWG Products.
- View Across All User Activity: Web, Application, DLP, Bandwidth, Email, and Malware in One View.
- Live Threat and Bandwidth Dashboards.
- Bandwidth Head Map Technology.
- Instant URL/Ad-Hoc Reporting Capabilities.
- A Dynamic Drill-Down Interface.
- Mobile Device Threat and Activity Reporting.
- Site Callout Capabilities.
- Automated Report Scheduling.
- Compliance-Reporting and Automated Backups.
- Consolidated Reports Across a Distributed Enterprise.

The iboss Difference – Not Just What, But Who and Where

Cyber threats, including malware and data loss — along with new potential of network peripherals "phoning home" — are constant security game-changers because they're continually growing in sophistication. As such, these menaces have eroded and will continue to compromise the effectiveness of current log-based threat detection and reporting. iboss SWG Threat & Event Console alters how we approach threat identification and mitigation by looking at your connection source and then identifying to whom and where you're connecting. With exclusive features such as threat GeoMapping and heat maps technology, iboss SWG Threat & Event Console provides instant visual insight to pinpoint threats across a global map. This system increases insight, shortens mitigation response, and reduces the total cost of ownership (TCO).

For more product details, see the iboss SWG Threat & Event Console Brochure.

iboss SWG Web Security Feature List

Threat Management

- HTTP/S Filtering
- Signature and Heuristic Application Filtering
- Dynamic Proxy Detection
- Filter Across 65K Ports

Platform

- Secure Linux OS
- Standards-based Fail-over
- Available Fail-Safe Bypass Ports

Configuration & Deployment

- Full Throughput Capabilities
- High Performance Transparent Inline Filtering (Not Proxy)
- Explicit Proxy Mode
- Inline Proxy Mode
- Switch With Multi-Link Trunking (VLAN Trunking Support)
- Hybrid Mode (Fixed Filtering, NTLM, and Proxy Authentication)
- Software Free Installation
- Operating-System Independent
- Web-Browser Independent

Authentication

- Single Sign-On Active Directory, LDAP and NTLM Integration
- Open Directory, eDirectory Open LDAP Integration
- Transparent Authentication for Apple/Mac Devices (Hook)
- Forced Authentication for Wired/Wireless Devices
- Individual User Login Creation (SuperUser)
- No Software/Thin Client Deployment Required for Directory Integration

Management

- Delegated Access to Filter and Reporter
- User/Group/IP-based Policy Management
- MAC-based Policy Management
- Web-Based and Remote Management
- Restore and Backup Settings
- Centrally Manage and Sync Multiple On-Premise Units (Cloud)

Infection Access Prevention

- Drive-by Spyware Protection
- Blocks Sites Infected With Malicious Mobile Code (MMC)
- Protection Against Phishing and Pharming Attacks
- Real-Time Security Updates to Database
- Blocks Spyware and Keylogger Back Channel Communication
- Data Loss Prevention (DLP)

Bandwidth Throttling

- Binds to Directory (AD, eDir/Open Directory)
- Throttle/Prioritize Traffic by Directory Group or User
- Apply Rules Using Predefined Categories (i.e. Streaming Radio)
- Throttle/Prioritize UDP, IP Range, TCP/IP
- Ensures Network Critical Traffic is Available while Recreational Traffic is Reduced During Peak Hours

URL Filtering

- 15+ Million Websites in URL Filtering Database
- 75 Web Categories in URL Database
- HTTP/S Filtering Transparently and Dynamically
- Hybrid Cloud Dynamic Database Updates 24/7/365
- Granular URL (i.e. Block YouTube, Allow Specific Videos)
- Block Page Override Through LDAP Specific to Machine
- Restrict Use of Keywords
- YouTube Video Library. Accessed On/Off Premise (Cloud)
- Delegated Media Library Management (i.e., YouTube)
- URL Exception Request Manager
- Social Network Access Control (Allow Facebook, Block Posting)
- URL Override to Domain
- Allow/Block List Import
- Restrict Domain Extensions
- Sleep Schedules
- SafeSearch Enforcement Dynamic Glype Proxy Detection

Web 2.0 Application Filtering

- Layer 7 Filtering
- Signature/Footprint Analysis Heuristics
- Advanced Google/YouTube Management Suite
- Control IM (AOL, Yahoo, MSN, Google, Camfrog, Jabber, and more)
- Blocks P2P (Gnutella, BitTorrent, eDonkey, Kazaa, Skype, and more)
- Blocks Proxy Avoidance Communication
- Detect "Rogue" Connections, Non-Standard Web Surfing
- Signature-Based Control of UltraSurf and Hotspot Shield
- High-Risk Application Quarantine

Reporting

- Delegate Report Access to Local Levels (i.e., H.R.)
- Auto-Record User Desktop on Threshold (Stored Locally)
- Live Desktop Stealth MultiView
- Store Locally All Network Activity for up to One Year
- Dynamic GeoMapping Technology
- Packet and Connection Tracking
- Dynamic Access to All Locally Stored Reports
- Drill Down Daily Reports to Individual User Activity
- Forensic Search Capabilities With Dynamic Search Results
- Provides Search Strings
- Search All Data by Keywords With Wildcards
- Real-Time Top Bandwidth Consumers Monitor
- Automated Daily/Weekly/Monthly Reports (PDF, CSV, HTML)
- Reports User Name, IP (Source/Destination), Net Bios Name
- Auto-Generate PDF Reports on Schedules
- Distributed Reporting Provides Central Access to Multiple On-Premise Units (No VPN Required)

Proactive Threat Notification

*Notifies Delegated Admins of Threats Immediately via Email

- Set Category Violation Triggers by Group
- Auto Record User Desktop/s on Triggers
- Instant Alerts on Keyword/s at Group Level
- Instant Alerts when 'Rogue' Activity is Detected by User

Internet Content Filtering

iboss SWG Web Security provides URL filtering, including HTTPS traffic. By using a massive database of URLs that update in real time, this ensures accurate filtering takes place and the potential for "false positives" is mini- mized. URL filtering is combined with signatures and heuristics to properly identify encrypted applications regardless of the port or protocol being traversed

- URL Categorization: 75 categories that filter by URL or domain for granular policy implementation.
- Hybrid cloud database updates access locallly and pushes to the cloud database, ensuring real-time updates.
- Keyword filtering filters words and phrases from forums, blogs, searches, etc. High Risk and Wild Cards allow for instant notification via email to shorten responses to threat.
- Safe Search enforcement re-enables safe search on all major search engines including YouTube if disabled.
- Virus/Malware filtering provides real-time updates, protecting networks from the latest threats.
- URL vs. Domain filtering gives organizations access only to the value of each domain and restricts unwanted content.
- Keyword filtering allow filtering words and phrases from forums, blogs, searches, etc. High Risk and Wild Cards allow for instant notification via email to shorten responses to threat.
- Filter domain extensions and file extensions create an "allow only" list to customize network access with flexibility.
- Control access by directory or local group policy and implement time-based controls by time of day or day of week at the group level.
- Prevent data loss on social networking sites by controlling access within these sites, including posting and gaming while still allowing access to areas within these sites which require access by the organization.

Clean Access to YouTube and Google Image Searches

YouTube and Google provide access to content that is valuable to organizations but they also incorporate access that may be inappropriate. iboss provides "clean" access by:

- GoLiveCampus.com – a cloud-based service that provides dynamic YouTube.com while stripping comments and ads from these videos and enforcing safe search. Video library allows the creation of video/media libraries where limited access users can view only approved videos. Department heads can create channels to share videos with select users.
- CleanYouTube – Provides access to YouTube.com while enforcing safe search, removing ads and comments, and ensuring "clean" access to relevant data only.
- Clean Image Search– Beyond standard Safe Search, iboss filters the links that feed images missed by Google Safe Search, removing images in violation of the Internet use policy. Additionally, iboss will strip comments and links from image results.

Reporting

Analytics

iboss SWG Web Security provides network-transparent insight on all network traffic that traverses the network. Data is proactively indexed throughout the day, allowing for drill-down review and comparison. Organizations gain keen insight on trends and history for all usage including access, violations and bandwidth to identify threats and data leaks as well as to adjust Internet use policies.

- Daily drill down through all events to the individual users.
- Instantly compare between current data and local data stored internally for avg. of one year.
- Identify all bandwidth consumers.
- Instant access to all users up to one year stored locally.
- Identify trends, searches, and queries on forums, search engines, blogs, and more.

Forensic Report Searching

Transparently access any event on the network stored on board for up to one year. Results display instantly, allowing for more dynamic forensic searches on keywords, violations, activities, and usage. Callouts provide information on user search queries and exact URL accessed keywords on all events.

Search By:

- Keyword including wildcards.
- Users, Groups, MAC, Comp. Name, Source/Dest., IP, Category, Action, and Start/End Time.
- Dynamically search logs as far back as one year.
- Identify threats immediately and create automated follow-up reports on events.

Automated Reports

- Set up reports internally or to third parties. Reports by iboss sent automatically as PDF, CSV, or HTML.
- Select from automatically generated reports or fully customized reports.
- Create automated report tracking for specific events or users on the network. iboss will track and send reports automatically.
- Report on individual or groups' time use, percentage of time by category, bandwidth, cost analysis to the network, and more.

Real-Time Network Analysis

iboss SWG Web Security provides instant insight on all network traffic traversing the network. This includes current sites accessed, top consumers of bandwidth by user name, and trending.

Including:

- Live bandwidth currently consumed.
- Top 2000 bandwidth consumers.
- Currently accessed sites and applications
- Trends/Searches.
- Identify keywords and threats.

Trigger-Based Auto Desktop Recording

Combines dynamic database updates, layer 7 analysis, heuristics and signature

Application Control

iboss SWG Web Security filters through layer 7, including UDP and incorporates signatures to pattern-match applications. By using signature-based filtering, iboss ensures complete control of applications, including SSL-based applications and regardless of ports.

- Application Filter: Control applications traversing network and restrict or allow based on Active Directory/eDirectory Groups or Subnet/IP ranges.
- Allow or Restrict applications by time, day, or week, based on directory groups.
- Identify applications, including those hopping ports through SSL, utilizing signatures.

Filter Avoidance Controls

- By combining dynamic database updates, layer 7 analysis, heuristics- and signature-based filtering, iboss detects and restricts proxy avoidance tools across all 65K ports.
- Signature-based filtering to dynamically detect Glype and other proxies as they are accessed.
- Heuristics and signatures including rogue-encrypted connections and SSL domain enforcement detect advanced avoidance tools, e.g., UltraSurf and Hotspot Shield.
- Advanced email alerts send email notifications on thresholds and triggers to proactively identify real-time threats, reducing response time.

Delegated Access to Reporter and Filter

Delegation of reports and filter controls allow organizations to provide local access to detailed reports. This provides department heads the option to view and create specific reports throughout the day or week, providing more insight on activities within their department.

- Allow access to filter or create reports by directory group or users, as well as IP range.
- Gain insight with the live activity dashboard for each department.
- Create Ad-Hoc reports for specific request scenarios.

Flexible Directory Integration

iboss' unique ability to bind to multiple or mixed directories (AD, eD, OpenDir) against one appliance provides flexible integration in even the most diverse networks.

- No software, thin client, or proxy settings required at desktop for directory integration, providing seamless integration.

Bandwidth Prioritize and Throttling

iboss' Bandwidth Management module provides dynamic control of bi-directional traffic. Flexible rules allows users to limit or prioritize based on directory groups, users, or IP/Subnet. Also, selecting from predefined categories such as 'Audio/Video' provides more flexible rule implementation.

- Throttle or prioritize by directory groups or users – ensures select groups and users have access during peak hours.
- Select from predefined categories for ease of policy implementation in comparison to port-based bandwidth management.
- Throttle/Prioritize by domain, IP, Port/Protocol.
- Scheduling of bandwidth access.
- Ensure mission-critical access while restricting recreational access during peak hours.