iboss™
CYBERSECURITY

MobileEther™
Integrated Web Security and MDM

The exponential growth of mobile in the workplace has spawned a wide-range of devices, platforms and applications, creating challenges to securing the borderless network. Finding solutions that can extend cybersecurity across all mobile users while ensuring protection of the devices themselves is critical. iboss is the only Web security platform that secures both Web access and your devices, eliminating the need to procure a third party solution. iboss' patented technology extends this comprehensive protection because it's the only cybersecurity solution that enables visibility and control over what's on the device, as well as what the device is accessing on the Web.

The iboss Advantage

The only solution offering visibility into Web and device security via a single real-time dashboard

- ✓ Combines enterprise mobile device management (MDM) and Web security in one platform for unsurpassed visibility across your organization with fewer resources
- ✓ Eliminates the need to purchase and manage third-party MDM solutions, resulting in a lower TCO
- ✓ Provides visibility and control over mobile application downloads via a real-time dashboard, increasing your ability to detect exploits and enforce regulatory compliance
- ✓ Removes blind spots by scanning mobile SSL/HTTPS traffic even when devices are off-premises
- ✓ Extends behavioral-based malware detection across mobile devices and remote sites, increasing your organization's security posture in minutes without costly CAPEX investments
- ✓ Provides full-featured mobile device management to protect your organization's data and devices

Feature Descriptions

iboss Cloud Web Security

iboss Cloud delivers Web security to all your mobile users, assuring compliance and efficiency across your organization:

- ✓ Detects and mitigates threats in hidden UDP ports with inline, stream-based technology providing visibility across all 131,070 TCP and UDP data channels on your network
- ✓ Provides a unified management console that secures across all platforms, Mac, iOS, Android, Windows, Google Chrome or mixed environments
- ✓ Offers unrivaled ease-of-use and lower TCO with centralized management and reporting via an intuitive interface encompassing BYOD and mobile users without the need to backhaul data to corporate HQ
- ✓ Extends iboss Cloud Advanced Threat Defense across all mobile and BYOD users
- ✓ Scans content in HTTPS/SSL across all mobile users to detect imbedded links, malicious code or access violations
- ✓ Delivers granular application management to ensure access to critical applications, while restricting unapproved applications, with controls applied by directory group or user membership

iboss
CLOUD

The iboss Cloud Platform deploys instantly to deliver iboss' patented next-gen technology direct-to-cloud, including our exclusive advanced threat defense features. With options for All-Cloud, Customer-Hosted Cloud, or any combination, you have maximum flexibility to meet your organization's requirements:

iboss Cloud – Unique node container architecture ensures your data is never mixed with any other organization's data.

Customer-Hosted Cloud – Deploy local sensors for some functions, while sending remote offices and roaming users direct-to-cloud with no backhauling data and no latency.

BYOD and Guest WiFi Management

iboss reduces the risks of BYOD and Guest WiFi users with integrated BYOD management that extends advanced threat protection across all your mobile users, including BYOD and guest WiFi, while ensuring that increased bandwidth demand doesn't impact mission-critical traffic. iboss also identifies BYOD users not using a NAC and provides a captive portal that binds them to your network directory or LDAP automatically, delivering accurate policy enforcement across all users. iboss BYOD tools include advanced application controls and High Risk Auto Quarantine.

MobileEther MDM – Optional Built-in Mobile Device Management

iboss MobileEther provides full MDM functionality, including locating devices with geomapping, remotely scanning and selectively wiping devices, and locking or pushing applications. Email trigger alerts provide insight on administrator-defined events, such as when a device leaves the network, when an unapproved app is installed, or if web access violations occur. There are 18 trigger settings that you can set to notify you of unauthorized activity. Features include:

- Easy over-the-air set-up and enrollment gets you started within minutes without requiring an Apple Configurator
- Social media controls enable flexible social media access based on directory group membership. Set policies per user including restrictions such as 'No Posting', 'Games' or 'Photo Uploads' to social media sites.
- Granular application management on mobile devices includes pushing customized apps, updating content on- or off-premises, restricting or allowing app store access and others.
- SSL scanning that monitors SaaS data transfers on any device to restrict high volume data movement from SaaS services.
- Easy authentication by binding devices to your existing directory services including Active Directory, eDirectory, Open Directory, and LDAP. Policies for Web access and mobile device profiles are based on directory profiles and consolidated through a central interface, simplifying setup, and maintenance.
- Accurate Policy Enforcement on Shared Devices by enabling dynamic changes to device settings including Internet access rules, device profiles, and APP store access. Policies are based on the specific user accessing the device, for accurate enforcement across shared devices.

Additional Features

- Options for All-Cloud, Customer-Hosted Cloud, or Combination
- Layer 7 Proxy circumvention defense
- Content-aware social media controls
- High-Risk device quarantine
- Content management for YouTube, Google images and translation
- Proactive threat notification with keyword and event triggers
- Granular bandwidth optimization to ensure mission-critical traffic
- Threat and Event Console Reporter integration
- Live dashboards track user events, threats, malware, bandwidth
- Trigger-based alerts
- Threat and bandwidth GeoMapping
- Single click policy management across mobile, BYOD, and wired devices
- Real-time off-premises policy updates
- Volume purchasing program management
- Secure sensitive documents on devices
- Filter Apple store apps by rating/age/type
- GeoMap device location on live map

For more information:

iboss Cloud Platform Data Sheet

iboss Secure Web Gateway Platform Data Sheet

About iboss Cybersecurity

iboss Cybersecurity defends today's large, distributed organizations against targeted cyber threats which lead to data loss, with the iboss next-gen Secure Web Gateway Platform, leveraging innovative cloud architecture and patented advanced threat defense technologies. iboss advanced solutions deliver unparalleled visibility across all inbound/outbound data channels, and include security weapons that reveal blind spots, detect breaches and minimize the consequences of data exfiltration. With leading threat protection and unsurpassed usability, iboss is trusted by thousands of organizations and millions of users. **Visit www.iboss.com.**