

# Mobile Security Solutions

## Next-Generation Security for the Borderless Network

The exponential growth of mobile in the workplace has spawned a wide-range of devices, platforms and applications, creating new challenges to securing the network. Finding solutions that can extend network security and include BYOD and mobile device management (MDM), is critical. Only iboss Mobile Security Solutions protect mobile users with next-generation technology that defends against advanced threats and zero-day attacks and prevents data loss, while assuring optimal network availability.

### Benefit Highlights

- Secures all users, on any devices or platforms, on or off premises with granular built-in BYOD and optional MDM
- Offers easy-to-use centralized management across mixed-mobile deployments
- Prevents unapproved apps with granular application management
- Assures network availability for large, distributed mobile deployments with Intelligent Bandwidth Management
- Consolidates detailed reporting and dashboards across all mobile users whether on or off the network
- Eliminates blind spots by scanning mobile SSL/HTTPS traffic even when devices are off-premises

### Feature Descriptions

#### Comprehensive Cloud Web Security

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

- **Unrivalled visibility across all 131,070 TCP and UDP data channels** on your network with inline, stream-based technology that detects and mitigates threats in hidden UDP ports.
- **Unified management console** that seamlessly secures across all platforms, Mac, iOS, Android, Windows, Google Chrome or mixed environments.

- **Ease-of-use and lower TCO** with centralized policy management and reporting. Secure on-network users through an appliance and then reconnect outside the network through cloud enablement.
- **Advanced threat defense** with integrated features that extend iboss Advanced Threat and Data Protection including Behavioral DLP and Sandboxing across all users.
- **Content scanning of HTTPS/SSL across all mobile users** to detect embedded links, malicious code or access violations.
- **Granular application management** assures access to critical

#### Deployment Options:

- ✓ Appliance
- ✓ Hybrid
- ✓ Cloud

#### iboss Mobile Security Suite Features

##### Advanced Mobile/ BYOD Security

- HTTP and HTTPS traffic Inspection
- Malware and botnet protection
- Data loss prevention on mobile devices
- High-risk user quarantine
- Granular bandwidth throttling to ensure mission critical traffic

##### Flexible Deployment & Administration

- Flexible Deployment, Windows, Mac, iOS, Android, and Chrome books
- Single click policy management across mobile, BYOD, and wired devices
- Real-time off-premises policy updates

##### Comprehensive Reporting

- Threat and Event Console Reporter integration across mobile/BYOD/MDM
- User and device activity reporting on MDM
- Live dashboards track user events, threats, malware, bandwidth
- Trigger-based alerts
- Threat and bandwidth GeoMapping

##### Built-in Optional MDM

- Remotely scan/selectively wipe devices
- Directory-based user authentication
- Create/push/restrict apps
- Volume purchasing program management
- Secure sensitive documents on devices
- Filter Apple store apps by rating/age/type
- GeoMap device location on live map

applications, while restricting unapproved applications, with controls applied by directory group or user membership.

- **Dynamic content awareness** detects suspicious behavior and mitigates risks in real time.

## Granular Bring Your Own Device (BYOD) Management

iboss BYOD management extends Cloud Web Security to your BYOD users by accurately identifying them on networks not using a NAC, and providing a captive portal that automatically binds BYOD devices to a network directory or LDAP. This enables group-based policies and enforcement, whether BYOD users are on wired or wireless devices. Features include:

- **Customizable captive portal automatically binds BYOD users** to directory services including Active Directory, eDirectory, Open Directory, and LDAP on wired and wireless connections for accurate user-based enforcement.
- **Unique location awareness** protects user privacy when they are off the corporate premises.
- **Operating System (OS) independence** provides flexibility to bind any device to the network.
- **High risk user quarantine automatically locks users** attempting illegal activity.
- **Ensures mission-critical traffic is not interrupted** by recreational BYOD traffic with the integrated Intelligent Bandwidth Shaper.

## MobileEther – Optional Built-in Mobile Device Management (MDM)

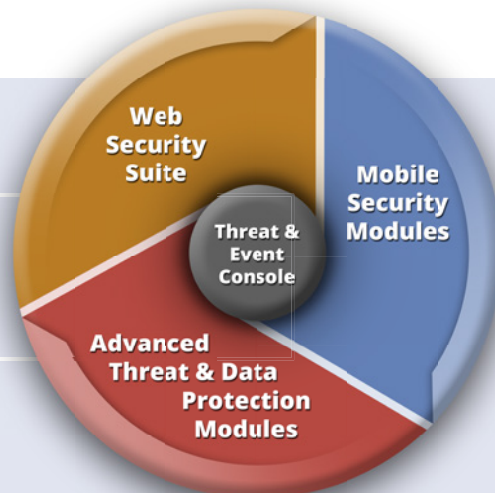
iboss integrated MobileEther MDM is an optional solution that offers all the features of traditional MDM, but extends protection to include Web security, intrusion detection and prevention, data loss protection, email security and comprehensive reporting, seamlessly integrated with the iboss Threat and Event Console. Features include:

- **Full MDM functionality such as locating devices** with geomapping, remotely scan/selectively wipe devices and lock or push apps. Email trigger alerts provide insight on administrator-defined events, such as when a device leaves the network, an unapproved app is installed, or Web access violations, with 18 trigger settings.
- **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 includes pushing customized apps**, updating content on or off premises, restricting or allowing APP store access and others.
- **Data loss prevention with SSL scanning** via MobileEther Behavioral DLP technology that monitors SaaS data movements on any device to restrict high volume data movement from SaaS services.
- **Secure, 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, which simplifies 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.

## iboss Next-Generation Solutions

iboss Network Security is a leading provider of innovative **Web Security, Mobile Security and Advanced Threat & Data Protection** Solutions. Backed by cutting edge technology built for Web 2.0 and beyond, with unparalleled visibility across all inbound/outbound data channels and port evasive applications.



[www.iboss.com](http://www.iboss.com) | +1 877.742.6832