MobileEther MDM

Features

- Directory Based User Authentication.
- User Authorization.
- User and Device Activity Reporting.
- Central Console to Manage Filtering and Reporting.
- Create Shared Content Apps for Organization.
- Volume Purchasing Program Management.
- Allow Delegates to Push Content to Other Organization Devices.
- Custom App Creation.
- Secure Sensitive Documents on Devices.
- Dynamically Filter Apple App Store by Rating/Age/Type.
- Geomap Device Locations on Live Map.
- Scan, Wipe, Push Apps.
- Manage App Delivery, Security, Updating.
- Push Services.

MobileEther

Mobile Device Security by iboss

Compliance Ready Mobile Device Management (MDM)

Issue: Your network is expanding it's use of mobile devices including iPads and Androids. The need for devices to meet regulatory compliance such as CIPA, HIPAA, PCI, and FISMA is eroding the effectiveness of traditional MDM. The necessity for these devices to be directory aware, secure against data loss, identify and mitigate malware and provide compliance ready reports are simply not found in traditional MDM offerings.

Solution: MobileEther MDM provides all key benefits of traditional MDM but expands security to encompass HTTP/S web filtering, intrusion detection and prevention, data loss protection, malware security, email security and compliance ready reporting. The MobileEther EMM security suite ensures mobile devices meet regulatory compliance and acceptable use policies. Simple integration with over-the-air deployment combined with compressive security suite reduces the total cost of ownership (TCO). MobileEther MDM extends mobile device security where MDM leaves off.

Unmatched visibility and easy enrollment for a mixed-device deployment.

Key Compliance Benefits: CIPA, HIPAA, PCI, SOX, and FISMA

- Provide HTTP/S web filtering with flexible user access and directory integration.
- Identify and secure unencrypted sensitive data transmissions including credit card information or social security numbers and provide detailed reports.
- Scan traffic for embedded threats including malware, botnets, new and unknown threats to prevent exploits.
- Sophisticated signature and heuristic based intrusion prevention and detection identify threats and anomalies, protecting the network and optimizing resources.
- Cloud based email security scans emails including attachments for viruses, malware, data loss, and protect against DoS attacks.

MobileEther MDM

Time and Money are Factors

To help you avoid the complications of setting up servers or spending days configuring devices, iboss MDM was designed with education in mind. It provides a cloud-based system that does not require any hardware onsite. Additionally, its simple 2-step setup allows configuration of devices even if they are not onsite. Remote devices are identified and automatically redirected for installation, which means a quick setup and minimal cost investment for you.

Uninterrupted Instruction

Ensuring fluid instruction minimizes distractions and frustration in the classroom. To achieve this, teachers can be provided tools to manage apps they find valuable for their students without having to wait for approval. In addition, collaboration with goLive! Campus and the integration of iTunes University with iboss MDM provides tools to share resources, discussion, videos and other learning material right in the classroom, uninterrupted.

More Inventory, Less Time

It's a reality — in today's education systems, the growth of education technology and the sheer number of devices and programs being used has expanded opportunities in education; but the staffing that's supporting educational technology has become restricted due to budget constraints. Devices such as iPads not only introduce a need to manage physical device inventory, but also software such as apps purchased for the district devices through the Apple Volume Purchasing Program (VPP). Going beyond physical device inventory, iboss MDM manages apps purchased through VPP, ensuring each license is utilized. Licenses on lost or damaged devices can be identified, minimizing cost and reducing waste.

Reports Take Center Stage

A key factor in managing devices and apps is identifying where they are and what's on them. Expanding general MDM reporting, iboss MDM focuses on the information you need to quickly resolve threats or compromised devices. Advanced reporting includes dynamic geomapping devices to identify where each device is currently and physically located over a live map and track lost/stolen devices quickly. Global app dashboard provides instant information on how many apps are installed on devices, apps by category, apps by age rating, and VPP purchased licensing. This ensures any unauthorized apps are quickly identified while also managing physical and software inventory. Reports are designed to identify the information you need when you need it.

Great (and Not so Great!) Apps

Simple access to apps for education, instruction and productivity is essential. Unfortunately, this also opens general access to the app stores' undesired apps. Managing what apps can be accessed is critical for smooth deployments as well as maintaining compliance with the AUP and CIPA. iboss MDM allows administrators to filter what apps are accessible and those restricted by group membership, providing security without compromise.

CIPA Compliance, on or off Premise

Seamless integration with iboss SWG Web Security creates central-Internet-access policy management and reporting whether devices are on- or off-premise. Information on all Internet traffic, including violations to the AUP, are logged and managed through the iboss SWG Web Security, providing detailed reporting for auditing, compliance and threat detection. iboss MDM integrates into the full suite of iboss SWG products securing networks on or off premise.

iboss MDM manages access to the app store by category, age rating, etc, increasing flexability when managing apps to all devices.