MobileSHIELD™
SOLVE BYOD

PC | Laptop | Mobile | Tablet

Control and secure mobile devices connected to corporate networks.

SnoopWall's patented MobileSHIELD agent is deployed and administered via the NetSHIELD Command Center. MobileSHIELD ensures BYOD flexibility by enabling owner control over device settings, applications and application privileges while not connected to corporate network resources. Administrator control over device settings, applications, application privileges, ports and mobile data connectivity is defined and enforced while mobile devices and tablets are connected to corporate networks. MobileSHIELD may be deployed on any mobile device or tablet or installed on laptops and PCs to enhance corporate IT security oversight and control.

The convergence of consumer privacy and mobile business security has arrived.

KEY FEATURES

- Smartphone & Tablet Protection
- Policy-based Mobile Security
- Hardware Port Protection
- App Level Firewall Defense
- Untrusted App Blocking
- Malicious App Logging
- Keyboard & Storage Encryption
- Microphone Eavesdrop Blocking
- Webcam Picture & Video Blocking
- Rogue Network Traffic Blocking
- Cloaking Data Against Theft
- Anti-espionage Protection
- Invisible User Management
- Rapid Onboarding & Deployment

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com

SW-MS-DS-2016-0224

MobileSHIELD™
SOLVE BYOD

The MobileSHIELD agent will run in one of two modes:

As configured by corporate IT

As configured by device owner

MobileSHIELD is a lightweight and flexible endpoint agent that works in conjunction in NetSHIELD to deliver security and eliminate data leakage while mobile devices are connected to corporate network assets.

MobileSHIELD is installed via a captive portal which defines BYOD policies and enables installation of the MobileSHIELD agent.

MobileSHIELD (Restricted Mode)

Device Privilege Flexibility - Ensures corporate IT control while connected to corporate network and owner control when not connected.

Asset Scanning - Identify rooted devices, developer settings, Android Debugging Bridge (ADB), lapsed OS and application updates and more.

Application Control - Manage application privileges including port access to control data leakage.

Port Control - Manage port access including Bluetooth, NFC, Mobile Data, GPS, Camera & Microphone.

Device Blocking and Monitoring – Control device privileges as administratively aligned to asset scan risk conditions.

Notifications – Configure notification settings for administrators and device owners.

Broad Platform Support - Including Android, iOS and Windows phones.

GET IN TOUCH

Toll Free: 1-800-991-3871 x1000 www.snoopwall.com securitysolutions@snoopwall.com