powerbroker® mobile

beyondtrust®
securing the perimeter within

PowerBroker® Mobile

Mobile devices are increasingly being used in environments that pose a great risk of data loss and vulnerability. The modern mobile device eco-system involves a device that has personal and company data on it along with third-party apps. This device by nature is truly mobile and can at anytime be connected to third party networks and public wireless networks. The risks to the device, data, and ease of access warrant configuration compliance, vulnerability assessment, and even the capabilities to remotely wipe the device in case of accidental loss or theft.

PowerBroker Mobile represents the next generation of mobile device management, providing remote administrative functions, configuration compliance, and vulnerability management for apps and mobile operating systems. The solution easily integrates management functionality with security information for your organization, providing security management and intelligence for BYOD environments and corporate devices.

Why PowerBroker Mobile?

- Easy deployment - Register device in seconds via automated emails
- Complete mobile device provisioning and configuration*
  - o VPN (PPTP, IPSEC) configuration
  - o Email accounts
  - o Exchange (IMAP/POP) accounts
  - o WebDav
  - o Password policy
- Enforce security policy
  - o Password complexity
  - o Encryption policy
  - o Time to lock
  - o Max failed password attempts
- Security actions
  - o Remote lock
  - o Remote wipe
  - o Last check-in time and GPS location
- Rule-driven actions
  - o Governance - gap in check-in times
  - o Compliance - policy compliance issues
  - o Risk - permission level adherence*
- Additional administrative alerts:
  - o User registration
  - o New device enrolled
- Integration with Retina CS
  - o Reporting
  - o Vulnerability management
  - o Asset tracking

*** Not supported on all mobile devices**

Complete device provisioning with PowerBroker® Mobile

PowerBroker Mobile contains key features that integrate mobile device management and security:

Key Benefits

— User-definable rules and actions based on Device Threat Score

— Mobile Connector to Retina CS for asset and vulnerability assessment

— Operating System profiling to determine when a device requires updating

— Modern web dashboard to view assets and applications by Risk, New Devices, Dormant, Update Available, or even potentially rogue connections

— Application permissions to critical device API's and functions*

— SaaS based solution handles mobile devices within your infrastructure, as well as operating outside of your perimeter

Platforms Supported

Android

- o 2.2.x / 2.3.x (Basic MDM Support)
- o 3.x/4.x (Enhanced Password policy)

Note: Device needs a valid Google/Android user account in order to activate push notifications (C2DM)

iPhone

- o **iOS 4 +**

Visit BeyondTrust.com for more information