

# ForeScout Mobile

ForeScout Mobile™ is the easiest, most flexible way for IT security managers to say “yes” to personal mobile devices on the enterprise network without compromising security. ForeScout Mobile works with ForeScout’s leading network access control (NAC) platform, ForeScout CounterACT, to provide real-time visibility and control of everything on the network—wired and wireless, managed and unmanaged, PCs and handheld devices.



## Challenges of Securing Mobile Devices

Gone are the days of standardized PC configurations, all managed and locked-down by the IT department. Now, you are dealing with a multitude of endpoint devices, most owned by the organization, and many owned by employees. Increasingly, employees are bringing their own personal devices—PCs, Macs, smartphones and tablets—into the office and connecting them to your network. Some people call this phenomenon the “Consumerization of IT”. Others call it “BYOD”. If you are responsible for security, you call it a nightmare.

Clearly, mobile computing devices introduce risk, especially the risk of data loss, unauthorized use, and mobile malware.

No matter where your organization is on the consumer IT adoption spectrum—blocking, tolerating, supporting or promoting the use of personal mobile devices—you need a way to enforce security policy. You need real-time visibility and control over your network and the mobile devices connected to it.

## ForeScout Mobile Benefits

ForeScout Mobile provides an automated, extensible and flexible approach to enforce security policy across a diverse array of corporate and personal mobile devices. ForeScout Mobile, working with ForeScout CounterACT, provides unified security management for everything on your network regardless of the type of device (PC, Mac, Linux, tablet, smartphone), the type of connection (wired, wireless, VPN) or the ownership of the device (corporate or personal). Benefits include:

- » **Visibility** - Identify all devices on your network in real-time, including personal devices without any agents installed. ForeScout CounterACT categorizes devices by type—Windows, Mac, Linux, Apple iOS, Android, Blackberry, printers, etc. ForeScout CounterACT also categorizes devices by ownership, e.g. corporate devices vs. personal devices. With ForeScout Mobile, you get additional detailed information about each mobile device including its configuration, its applications, and its security posture.
- » **Policy enforcement** - ForeScout CounterACT lets you enforce any type of network access policy you may wish. You may choose to prohibit unauthorized users and mobile devices on your network. Or allow some (or all) users and mobile devices, but limit them to specific portions of your network. With ForeScout Mobile, you can enforce granular network access policies, and you can directly manage the configuration of supported handheld devices.
- » **Security** - By itself, ForeScout CounterACT provides strong network access control and protection against attack by personal mobile devices. With ForeScout Mobile, you get extra security for supported handheld devices such as: remote wipe; enforce password policy; require apps such as anti-virus, MDM or virtualization; remove or disable native apps such as the camera.

## ForeScout Mobile Features

### ForeScout Mobile Features

- » Identify corporate vs. personal devices
- » Identify unauthorized and non-compliant devices
- » Identify mobile devices without password protection
- » Identify rooted devices and jailbroken devices
- » Identify mobile devices that are missing required apps, for example, corporate, MDM or security apps
- » Send messages to mobile users
- » Block or limit network access based on who, what, when, where, and how the device is configured
- » Unified management and reporting of all endpoint devices on the network regardless of user, device ownership, device type, connection method, or location
- » Identify and block malicious activity



*ForeScout Mobile provides role-based network access control and automated guest registration.*

## How ForeScout Mobile Works

ForeScout Mobile is a family of plug-in modules that augment the capabilities of ForeScout CounterACT. The modules include: ForeScout Mobile Security Module and ForeScout Mobile MDM Module.

### ForeScout Mobile Security Module

The ForeScout Mobile Security Module for Android is a ForeScout CounterACT plug-in and a lightweight app for Android devices. The app collects hardware, software and configuration information for each device on which it is installed and reports this to the ForeScout CounterACT appliance. This allows ForeScout CounterACT to determine the security posture of the Android device and restrict network access on the basis of that information.

ForeScout Mobile Security Module for iOS natively supports iOS devices, such as the iPad and iPhone, by employing the Apple Mobile Device Management API and the Apple Push Notification service (APNs) which are built into the iOS 4 operating system. Hardware and software details are collected by the iOS device and delivered to the ForeScout CounterACT appliance. Actions such as lock, password change, full wipe, and selective wipe of corporate data can be pushed to the iOS device along with custom iOS profiles. No agents are required on the iOS device.

Together with ForeScout CounterACT, ForeScout Mobile Security Module:

#### Identifies and categorizes all personal devices

- » Detects all devices on your network in real-time, regardless of the connection method—wired, wireless, or VPN.
- » Categorizes devices by type—computers, wireless access points, handheld phones, USB connected devices, printers, gaming consoles, etc.
- » Categorizes devices by operating system—Windows, MacOS, Apple iOS, Android, Windows Mobile, Blackberry.
- » Categorizes devices by ownership. Built-in mechanisms allow ForeScout CounterACT to distinguish personal or unknown devices from corporate devices.

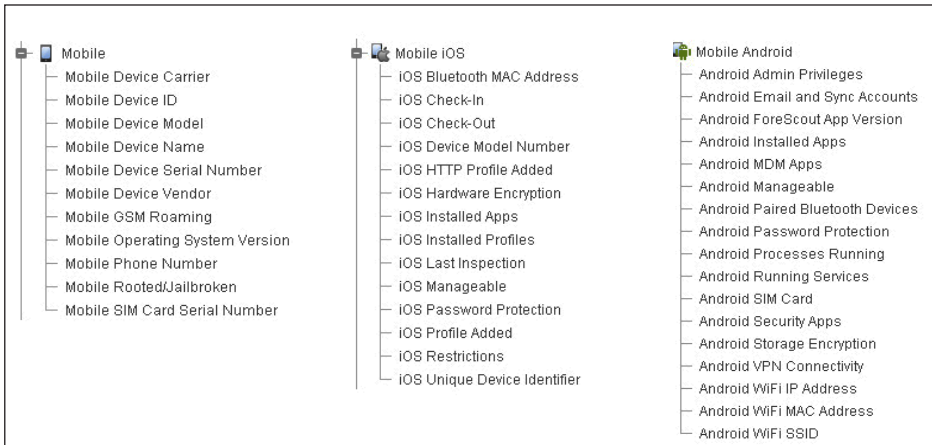
#### Provides detailed information about iOS and Android devices

- » Hardware information such as vendor, model, OS version, installed apps, IP and MAC addresses, serial number
- » Is the device jailbroken or rooted?
- » How is the device connected? WiFi? VPN? Broadband?
- » Is password enabled?
- » Is encryption enabled?
- » What applications are installed?
- » Are security applications such as antivirus or MDM installed and running?

#### Offers broad enforcement options

- » Monitor - learn who and what are on your network, and identify non-compliant systems
- » Notify - send emails or messages to IT personnel or end-users, or HTTP hijack end-users. Automated messages can guide end-users to take remediation steps, such as install specific MDM applications or security tokens.
- » Limit - limit the network access based on device type, device ownership, time of day, and device compliance. The limited access network can include a subset of applications and data, blocking access to more sensitive corporate resources.
- » Block - keep all (or just certain types of) devices off your network completely.
- » Remediate - directly remediate (without end-user intervention) iOS devices with actions such as remote wipe; enforce password policy; require apps such as anti-virus, MDM or virtualization; remove or disable native apps such as the camera; and enforce specific WiFi access methods.

**Protects your network from attack.** ForeScout CounterACT includes ForeScout's patented ForeScout ActiveResponse™ technology which blocks both known and unknown attacks without signatures. If any device on your network begins to attack your network, probing for weaknesses or trying to propagate, ForeScout CounterACT detects this and will thwart the attack and quarantine the malicious device from your network. This patented threat prevention technology does not require signatures or any form of maintenance.



*ForeScout Mobile Security Module collects a wide variety of information from iOS and Android devices.*

## The ForeScout Mobile MDM Module

Even if you have already deployed or intend to deploy a mobile device management (MDM) system, you still face security gaps unless you have direct control over all network access. With ForeScout Mobile MDM Module, security teams can achieve network access control and greater operational efficiency by merging NAC and MDM security functions, enabling unified access control policies not available in MDM, and negating the need for security managers to use an MDM console.

The ForeScout Mobile MDM Module allows you to leverage your existing MDM solution within the broader context of unified security control that CounterACT provides. The module instantly brings comprehensive information about all MDM-managed mobile devices to the CounterACT appliance, where the information is displayed alongside information about unmanaged mobile devices and devices that are outside the scope of your MDM system (such as PCs). From the CounterACT console, you can configure and enforce security policies, monitor and report on policy adherence, and remediate devices supported by your MDM system.

The ForeScout Mobile MDM Module, an optional plug-in for ForeScout CounterACT, is sold separately. The ForeScout Mobile MDM Module will be available in mid-2012.

When used in conjunction with your existing MDM system, ForeScout CounterACT with ForeScout Mobile MDM Module provides:

- » Improved security by blocking unauthorized users and devices from the network
- » Enhanced mobile device security by identifying malicious behavior
- » Extended visibility by detecting unmanaged devices on the network
- » Unified policy management and compliance reporting for all endpoint devices—PCs, smartphones, and tablets
- » More automated installation of MDM apps, VDI apps and other mobile apps by automatically directing unmanaged devices to a corporate app store or web page

## ForeScout Mobile Features (continued)

### Features Specific to ForeScout Mobile Security Module

- » Remediate iOS devices including remote lock, full wipe, selective wipe, passcode enforcement, other device restrictions
- » Configure corporate email on iOS
- » Configure enterprise resources such as WiFi, VPN, proxy server, AD and PKI on iOS devices
- » Remediate Android devices by setting password, set encryption, and kill app

### Features Specific to ForeScout Mobile MDM Module

- » Collect detailed device information from the MDM system
- » Trigger device remediation using the MDM system (specific remediation features vary depending on the MDM system)

## The ForeScout Difference

Unlike typical mobile security solutions, ForeScout CounterACT with ForeScout Mobile provides:

- » Improved security by blocking unauthorized users and devices from the network.
- » Improved visibility by detecting unmanaged devices on the network
- » Unified security management for everything on your network regardless of the type of device (PC, Mac, tablet, smartphone), the type of connection (wired, wireless, VPN) or the owner of the device (corporate or personal)
- » Cost savings. The 3-year cost of ownership of ForeScout CounterACT and ForeScout Mobile is typically a fraction of the cost of an MDM solution.
- » Easier deployment and a better user experience than VDI systems or sandboxing systems

## Device Support

ForeScout Mobile is a series of plug-in modules that install on ForeScout CounterACT physical or virtual appliance.

- » ForeScout Mobile Security Module for Android includes an Android app that natively supports Android version 2.1 and above.
- » ForeScout Mobile Security Module for iOS natively supports iPad and iPhones running iOS version 4.0 and above.
- » ForeScout Mobile MDM Module will be available in Q3 2012. For information on which MDM systems will be supported by the ForeScout Mobile MDM Module, please visit [www.forescout.com](http://www.forescout.com) or contact us via phone 1 (866)-377-8771 or +1 (408) 213-3191.

## Tiered Mobile Security

ForeScout provides IT organizations the means to cost-effectively offer a tiered level of service to meet the needs of mobile users throughout the organization. You may choose to deploy all three solutions, reserving the more expensive solutions for high-value users and devices.

	<b>ForeScout CounterACT</b>	<b>ForeScout CounterACT + ForeScout Mobile Security Module</b>	<b>ForeScout CounterACT + ForeScout Mobile MDM Module + 3rd Party MDM System</b>
<b>Application</b>	Guest network access plus enforcement of basic network access control policies based on the type of device and the user.	Adds the ability to enforce network access policies based on the security posture of iOS and Android devices. Adds the ability to manage compliance and configuration of iOS devices.	Adds the ability to manage compliance and configuration of all supported handheld devices. Adds uniform policy management for all devices (PCs plus handheld), managed and unmanaged.
<b>Usage</b>	Basic mobile security requirements	More advanced mobile security requirements	Extensive mobile security requirements, or for a select population of high-value users
<b>Price</b>	\$	\$\$	\$\$\$\$\$

## About ForeScout

ForeScout Technologies is a leading provider of automated security control solutions for Fortune 1000 enterprises and government organizations. With ForeScout, organizations can accelerate productivity and connectivity by enabling people to access corporate network resources where, how and when needed without compromising security.

ForeScout's automated solutions for network access control, mobile security, threat prevention and endpoint compliance empower organizations to gain access agility while preempting risks and eliminating remediation costs. ForeScout CounterACT has been chosen by over 1000 of the world's most secure enterprises and military installations for global deployments spanning 37 countries. The company delivers its solutions through its network of authorized partners worldwide. Learn more at <http://www.forescout.com>.



Scan this code with your smart-phone QR reader to get more info about ForeScout Mobile

