Network and Device Level Mobile Security Controls

IT Considerations in the BYOD Era

Scott Gordon CISSP-ISSMP

Vice President, ForeScout

June 14, 2012

ForeScout

"Bring Your Own Device" BYOD

Many things to many people

BYOD: the level at which an IT organization prohibits, tolerates, supports or embraces personal mobile device use in their company and the non-technical and technical controls used to enforce the policy

Question: is it about the user, device, network, connections, applications, privacy or data?

Answer: All the above – it's all interrelated

Policy needs to consider all the above

ForeScout

Policy Development

Define use cases first, tools later

Define and document mobility use cases

Involve relevant stakeholders

more efficient and better assures acceptance

- Business drivers
- User types
- Device and application use
- Use of an access to network resources
- Devices supported
- Data protection requirements
- Risks and legalities
- Control mechanisms
- Costs

ForeScout

Various Technical Controls

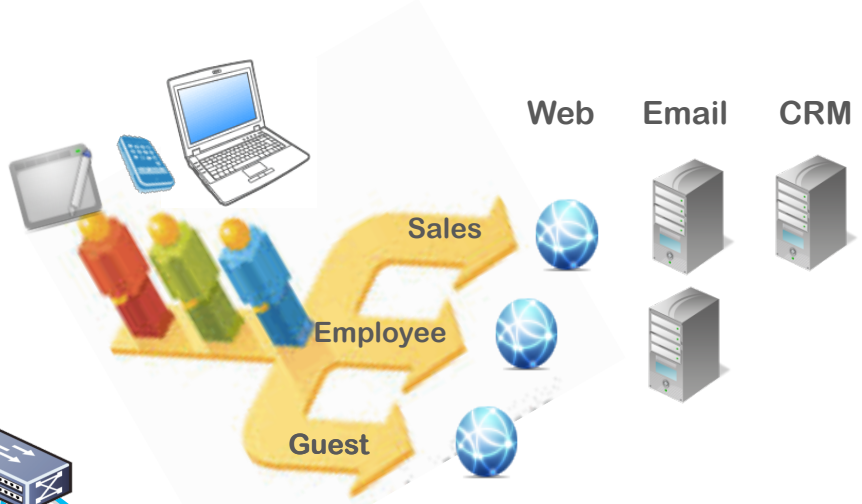
Most companies will use a variety of mechanisms

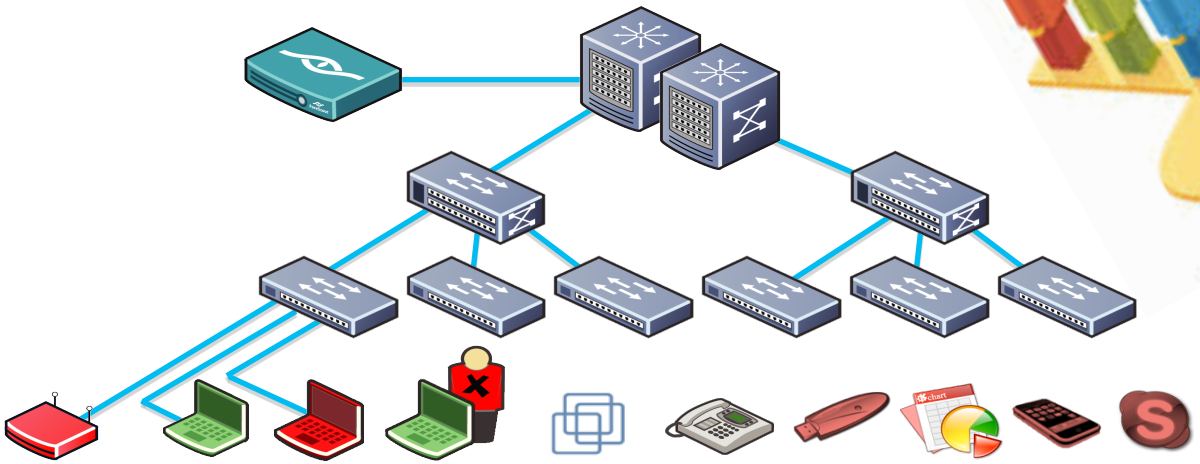
- Block all of the BYOD devices
- WAP – Wireless Access Point
- NAC – Network Access Control
- MDM - Mobile Device Management
- MAW - Mobile Application Wrapper
- MEAM – Mobile Enterprise Application Management
- Cloud / Virtual Data Store
- Cloud / Portals
- VDI - Virtual Desktop Infrastructure

ForeScout

NAC in Action

- **Who and what is on your network?**
- **Assess access credentials and endpoint security posture**
- **Allow, limit or block network access based on policy**
- **Remediate violations, fix endpoint compliance gaps and stop threats**





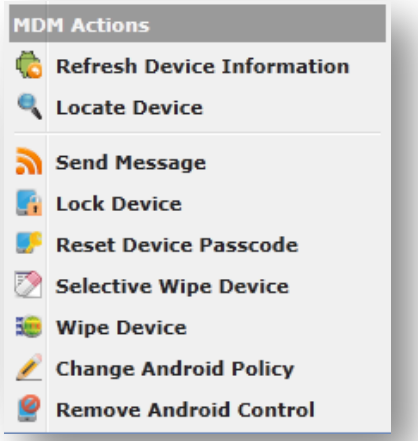
ForeScout

Mobile Device Management

Basic Controls

- **Device enrollment**
- **OTA configuration**
- **Security policy management**
- **Remote lock, wipe, selective wipe**
- **App portal**

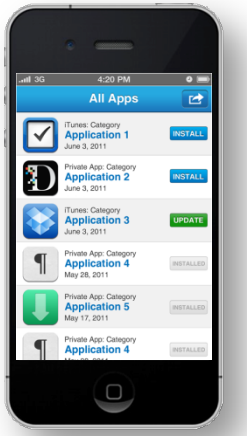
Device Enrollment, Acceptable Use



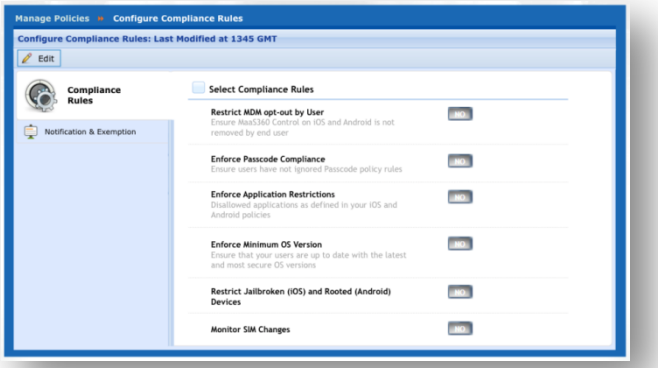
MDM Actions

Advanced Controls

- **Email access controls**
- **Application management**
- **Document management**
- **Certificate management**
- **Profile lock-down**
- **PII Protection**



Corp App Storefront

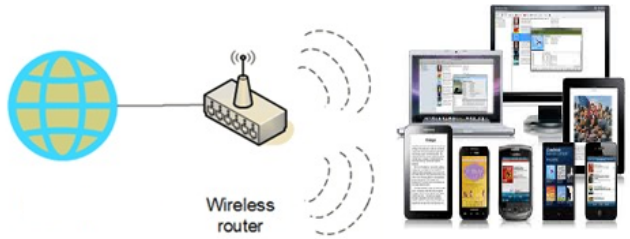


Event-based Security & Compliance

ForeScout

NAC+MDM Synergy for Mobile Security
Visibility, compliance and access control

NAC focus is on the network



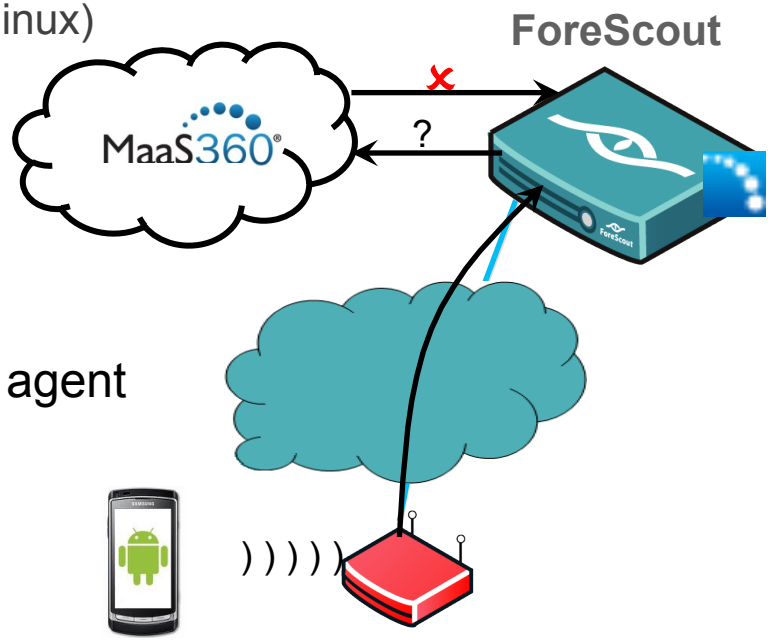
MDM focus is on the mobile device

Mobile Security	NAC Alone	MDM Alone	NAC+MDM
Visibility	Basic info on all mobile devices	Full info on only managed devices	Complete
Access Control	Partial (limited endpoint info.)	For managed and email only	Complete
Compliance	Limited	Managed only	Complete
Network control	Strong	None	Complete
Deploy Agent	Network based	Pre-registration	Both

ForeScout

Example: Automated Registration

1. Device connects to the network –
   a. Classify its type:
      Mobile device and its type (Android, iPhone iOS, Blackberry OS) or PC (Windows, Mac, Linux)
   b. Check if it has the mobile agent



2. If the agent is missing –
   a. Quarantine the mobile device
   b. Register and install relevant MaaS360 agent on the mobile device
      (via HTTP Redirection)

3. Once installed with an agent –
   a. Allow access based on policy
   b. Continue monitoring the agent's operation

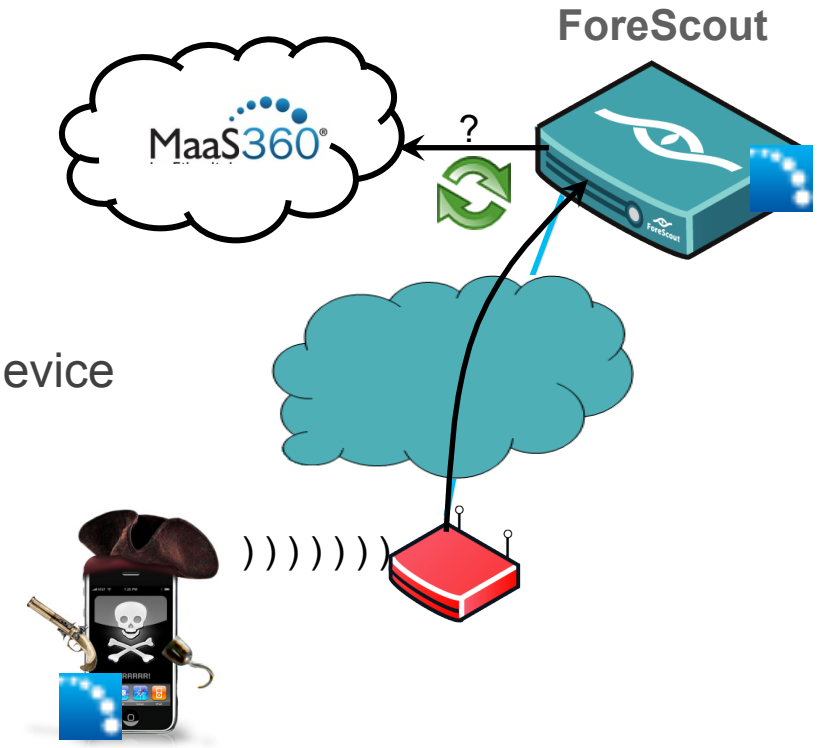
ForeScout

Example: Real-time Compliance Testing

1. Device connects to the network –
   Has a mobile agent but is jail broken

2. Force a compliance test
   a. CounterACT informs MaaS360 to assess configuration attributes
   b. If in violation, inform ForeScout CounterACT
   c. CounterACT quarantines the mobile device and sends informative message

3. Enable a compliance recheck
   a. CounterACT informs MaaS360 to test
   b. Upon re-assessment, allows onto network if violation no longer exists
   c. Continue monitoring the agent's operation



ForeScout

Thank you.

ForeScout Technologies - Automated Security Control

Enable Access Agility without Compromising Security

www.forescout.com