information
SECURITY
key to the business

BYOD and Mobile access

Oct. 18, 2013

What is BYOD?

- From Wikipedia
  - BYOD refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and use those devices *to access privileged company information and applications*.[

Why are companies doing this

Pro's

Cost Cutting: Employers may elect to offer little or no stipend for device and expenses.

Employee Satisfaction and Efficiency: Some employees prefer and are more effective with devices that are not the corporate standard.

Cool factor: Aside from their financial challenges, Blackberry has fallen out of fashion

Con's

Data compliance: How do do you assure compliance and customer confidence?

Ownership: if lost, stolen or employee leave company can you remote wipe all data or just corporate data?

Support Model: Help desks need to be well versed in multiple platforms and not just the corporate standard.

Some hard decisions were required

- Can you allow corporate data on personal devices?
- VPN or DMZ exposed services?
- Container or Native Apps?
- MDM or ActiveSync Policies?
- Do we support both iOS and Android?
- WiFi or 3G/4G

Some difficult answers were provided

- Can you allow corporate data on personal devices? kinda
- VPN or DMZ exposed services? DMZ
- Container or Native Apps? Container
- MDM or ActiveSync Policies? MDM ...kinda
- Do we support both iOS and Android? Both for now
- WiFi or 3G/4G? 3G/4G only

Why no WiFi?

- This was a very controversial decision for us but it was a matter of cost and equality
  - We have a lot of locations with relatively low bandwidth T1 or less
  - We were sensitive to not create an environment of haves and have not's
  - Cost prohibitive to scale bandwidth across the enterprise to support all use cases
- It's my opinion that users want the convenience of one device and access to their personal apps Facebook, Twitter, Instagram etc.. and the occasional use of corporate e-mail, calendar and intranet.

WiFi’s dirty little BYOD secret

- If you don’t actively control it determined users will find a way.
- If you only do 802.1x with username and Password you have a BYOD problem, you just don’t know it’s scale.

OK so now what?

- NAC has resurged as a device profiling and registration solution.
  - Cisco ISE, Foresout, Bradford Networks, FiberLink and others all offer solutions.
- Use what you already have to make after the fact decisions.
  - Correlate RADIUS servers logs and DHCP Server logs to identify rogue devices.

3 Lessons

1. Users want the native apps and not the container versions
2. Users want WiFi (3G iPad’s are expensive)
3. Your users will find use cases you never thought of as to why they need items 1 and 2

Questions??