Mobile Device Usage

Remeber This?

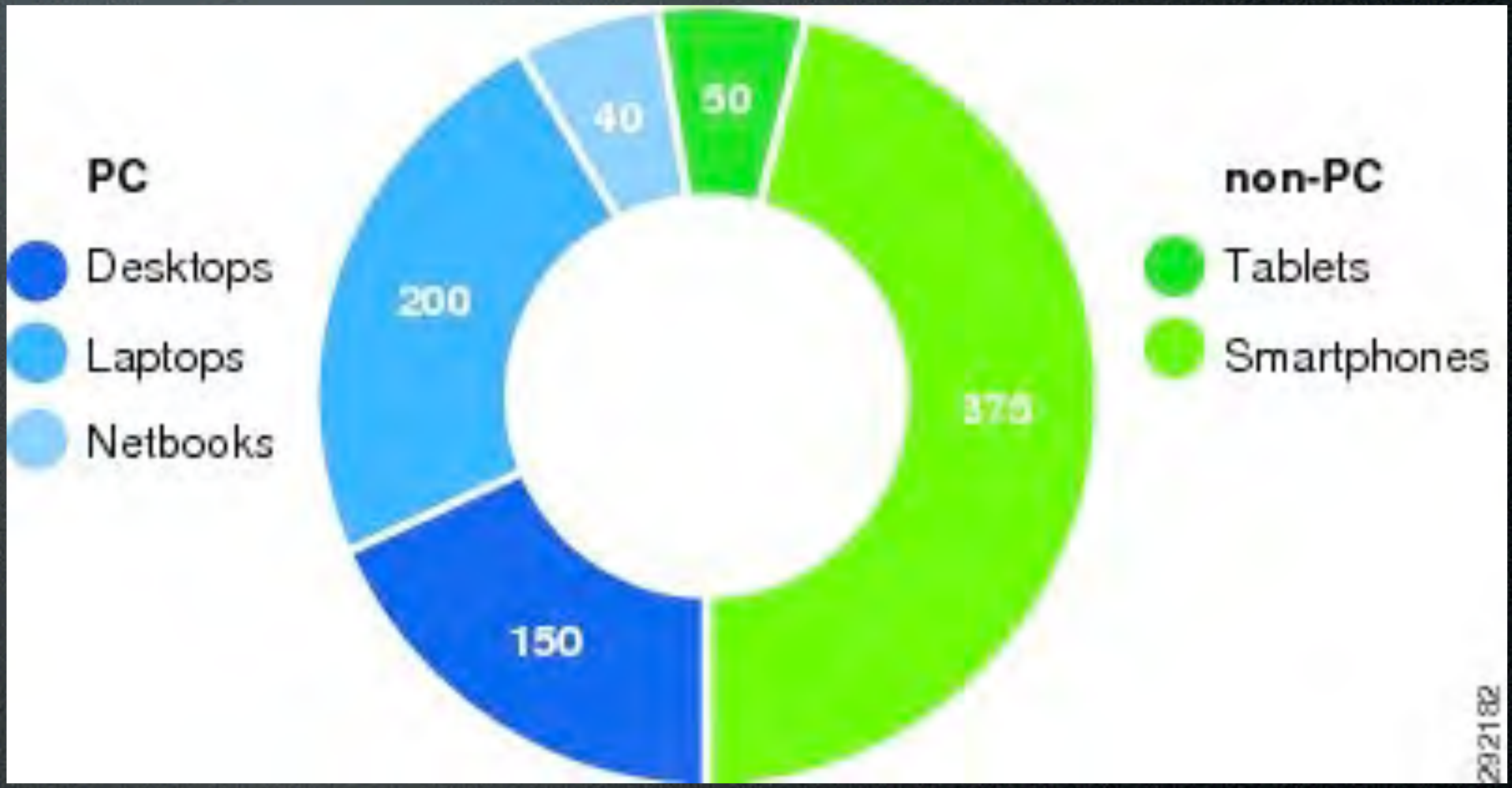
The original, live presentation
included the embedded video below:

http://www.youtube.com/watch?v=BO-nFt2mohI

A Changing Industry

- Proliferation of Smart Phones and Tablets.
- Quick poll?

PC and Non PC Sales, 2011 (millions)



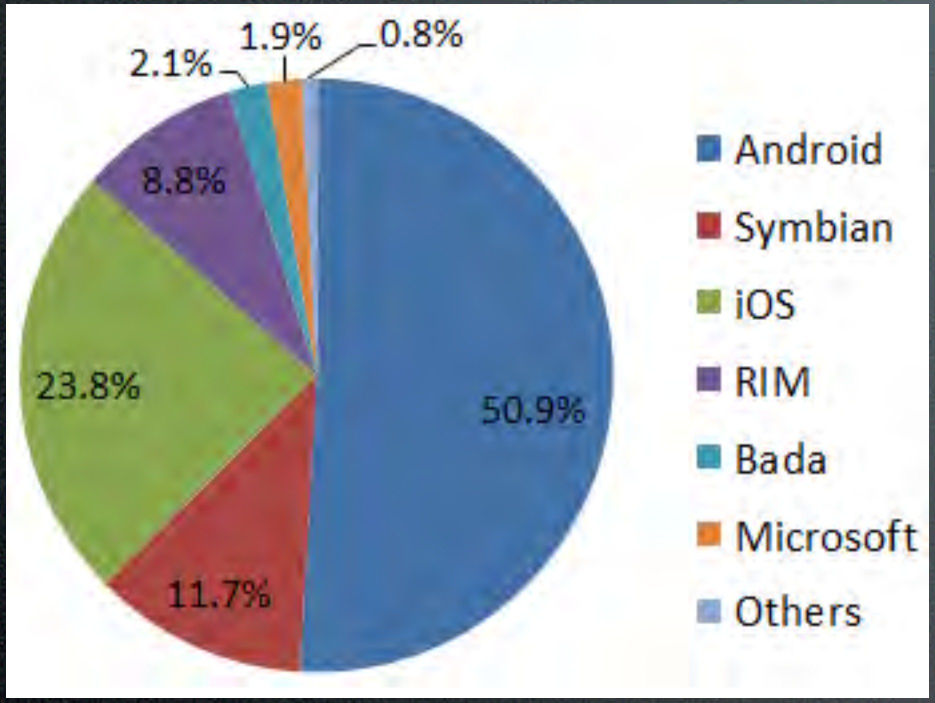
BYOD?

- BYOD = Bring Your Own Device
- Might also be called “Consumerization of IT”
- Roots in Education

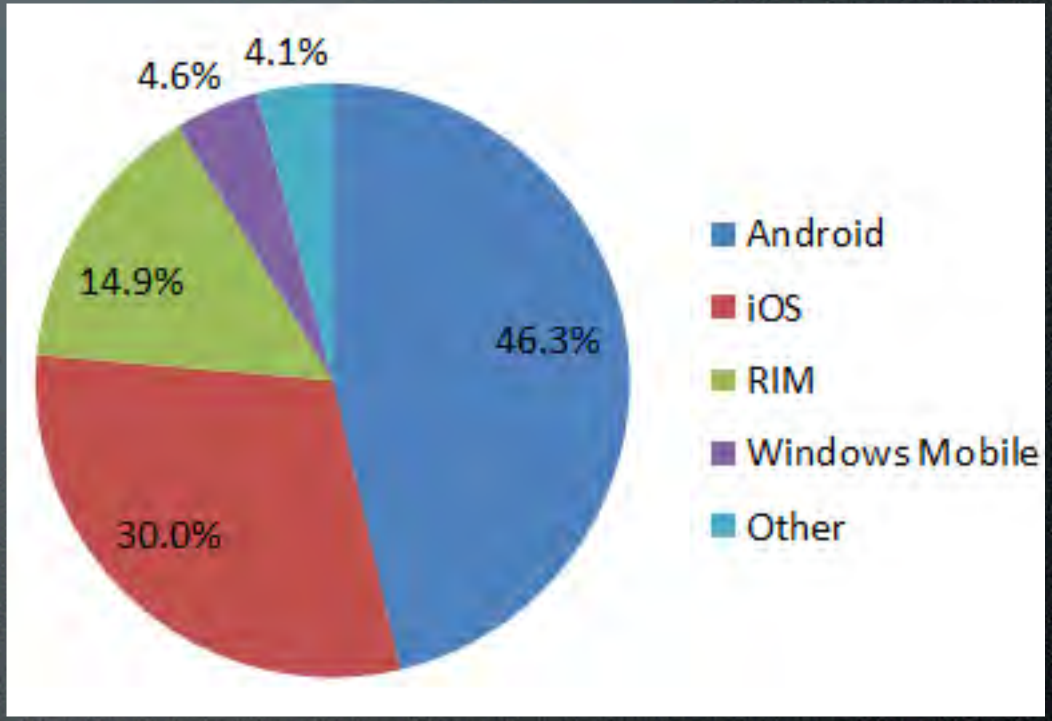
What is Driving BYOD

- New paradigms that change the way we compute such as touchable surfaces
- “Cool” devices that everybody wants
- Employee preferences

Device Distribution Q4 2011



Gartner



Nielsen

Other Drivers

- Technology savvy users
- Personal equipment is sometimes more current that IT provided gear
- Sophistication of home IT. It just kind of works.. Well.. Kind of..
- The work day has extended to home

Microsoft Ad - for all you IT Managers

The original, live presentation included the embedded video below:

http://www.youtube.com/watch?v=RzJwaEiAays&feature=related

Risk vs Reward

What does the Industry Think?

Which of the following do you believe is the most accurate statement about employees using personal mobile devices for work activities? (n=711)

a. The benefits outweigh the risks.	27%
[✓ b. The risks outweigh the benefits.]	[✓ 37%]

What does the Industry Think?

Which of the following mobile devices do you believe represents the greatest risk to your enterprise? (n=711)

a. Work-supplied smart phones	7%
b. Work-supplied laptops/netbooks	13%
c. Work-supplied tablet computers	2%
d. Work-supplied broadband cards	1%
e. Work-supplied flash drives	10%
f. Any employee-owned mobile device	58%
g. None of these pose significant risk.	6%
h. Other (please specify)	4%

What does the Industry Think?

If your organization allows personal smart devices (e.g., employee-owned smart phones or tablet computers) to connect to its networks and applications, what is its current security stance? (n=710)

a. We have a policy and systems to control all features on personal smart devices (including application installation and the ability to wipe all data). 13%

b. We have a policy and limited controls (such as encryption, password requirements and remote wipe capabilities). 22%

c. We have a policy and controls that allow for encryption, password requirements and management of organizational (non-personal) data on the smart devices. 15%

d. We have a policy, but do not control or modify personal smart devices that connect to internal systems. 14%

e. We do not have a policy or controls for personal smart devices that connect to internal systems. 10%

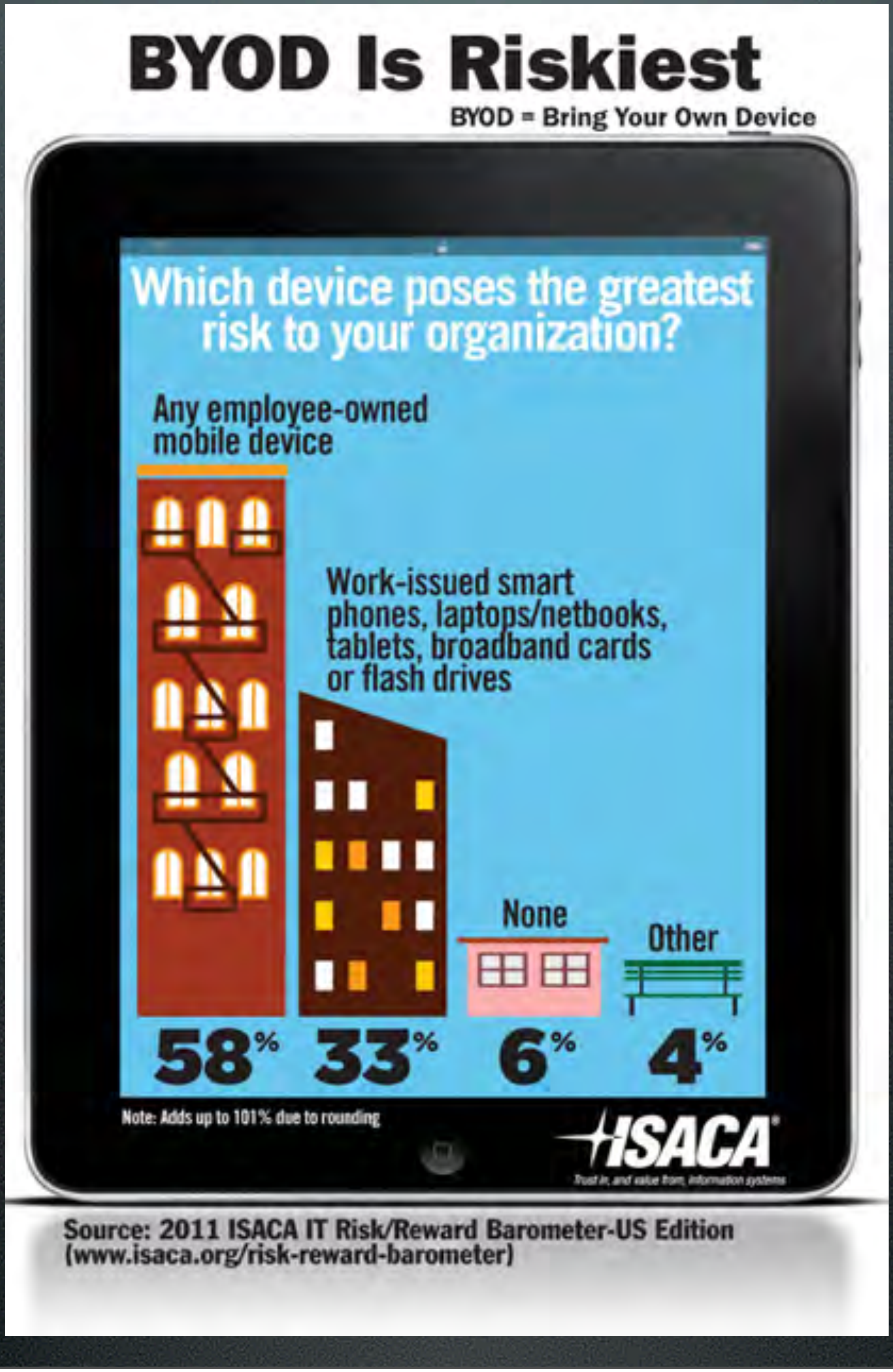
f. Not applicable 26%

What does the Industry Think?

What is the riskiest behavior you are aware of an employee doing with a mobile device that has access to the corporate network? (n=705)

a. Lose the device	27%
b. Disable the lock feature	4%
c. Keep passwords stored in a file or as a contact on the device	7%
[✓ d. Store company data in an unsecured manner]	[✓ 44%]
e. Access dangerous or risky web sites	8%
f. Leave Bluetooth or WiFi access on and unsecured	7%
g. Other (please specify)	3%

Conclusion



BYOD Is Riskiest

BYOD = Bring Your Own Device

Note: Adds up to 101% due to rounding

Source: 2011 ISACA IT Risk/Reward Barometer-US Edition (www.isaca.org/risk-reward-barometer)

Benefits of BYOD

- Cost savings by shifting hardware cost to user
- Cost savings by shifting service cost to user
- New features and capability can drive production
- Hardware updates happen more frequently that traditional IT
- Users generally always have their "work device" with them
- Increase employee satisfaction and productivity

Risks of BYOD

- Helpdesk impact - many more devices to support
- Many different OS and software packages to support
- Harder to enforce an acceptable use policy on a privately owned device.

- Compliance issues for data storage (PCI, DSS, HIPAA, etc)
- Co-mingled personal / business data
- Network security threats including viruses
- Wifi usage and capacity
- Dataloss or theft

Governance Policy

Policy Considerations

- Purpose – usually to protect confidential information and maintain information system security and availability.
- Applicability – Employees, guests, contractors. Types of devices.
- Threats – Loss, theft, copyright violations, malware, compliance.
- Access Control – device registration.
- Security – agreement to monitoring, access limits, locking, notification of loss.
- Support – which devices and applications will receive support.
- Charges and reimbursements – Limit on company payments.
- Lost or Stolen devices – what actions need to be taken by whom and when.

Policy Types

- Lock Down
- Wide Open Access
- Hybrid Approaches

The Lockdown Policy

The original, live presentation included the embedded video below:

http://www.youtube.com/watch?v=GYCduxWF8Yc&feature=related

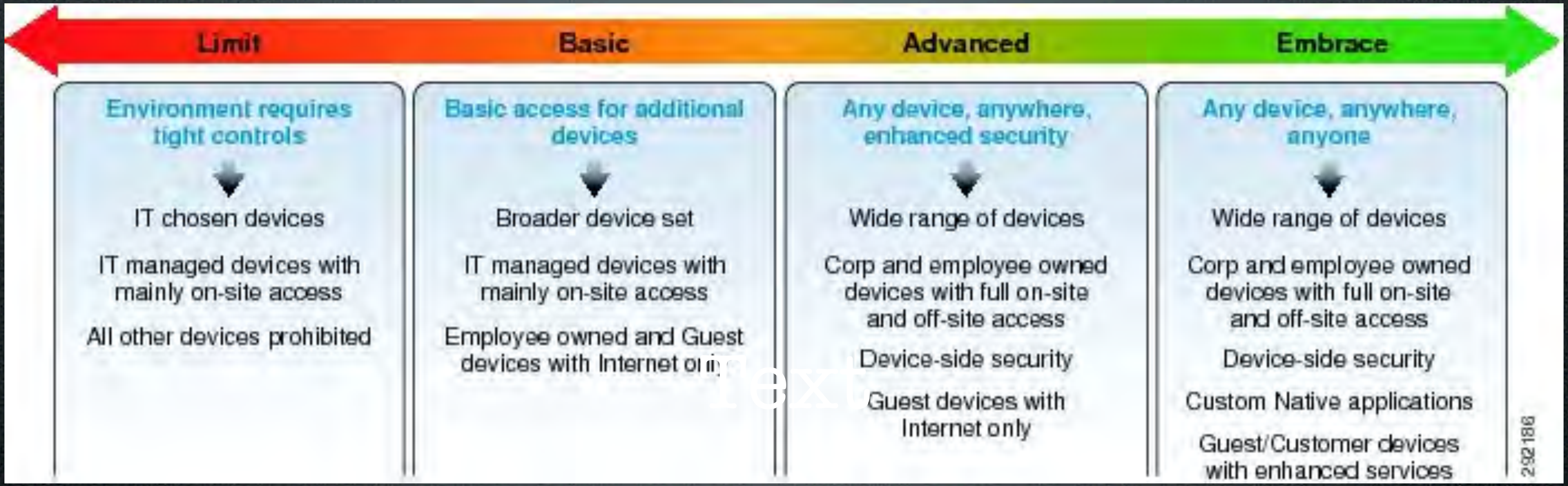
Lock Down

- Limited or no personal devices allowed
- Location restrictions (on-site only access)
- Unidentified or undefined usage not allowed.

Wide Open Policy

- All devices allowed
- General network access provided for all devices
- Access is provided by:
  - VPN
  - Internet facing applications
  - Native Device Applications
  - VDI

Hybrid Approaches



Limit	Basic	Advanced	Embrace
Environment requires tight controls	Basic access for additional devices	Any device, anywhere, enhanced security	Any device, anywhere, anyone
IT chosen devices	Broader device set	Wide range of devices	Wide range of devices
IT managed devices with mainly on-site access	IT managed devices with mainly on-site access	Corp and employee owned devices with full on-site and off-site access	Corp and employee owned devices with full on-site and off-site access
All other devices prohibited	Employee owned and Guest devices with Internet only	Device-side security	Device-side security
		Guest devices with Internet only	Custom Native applications
			Guest/Customer devices with enhanced services

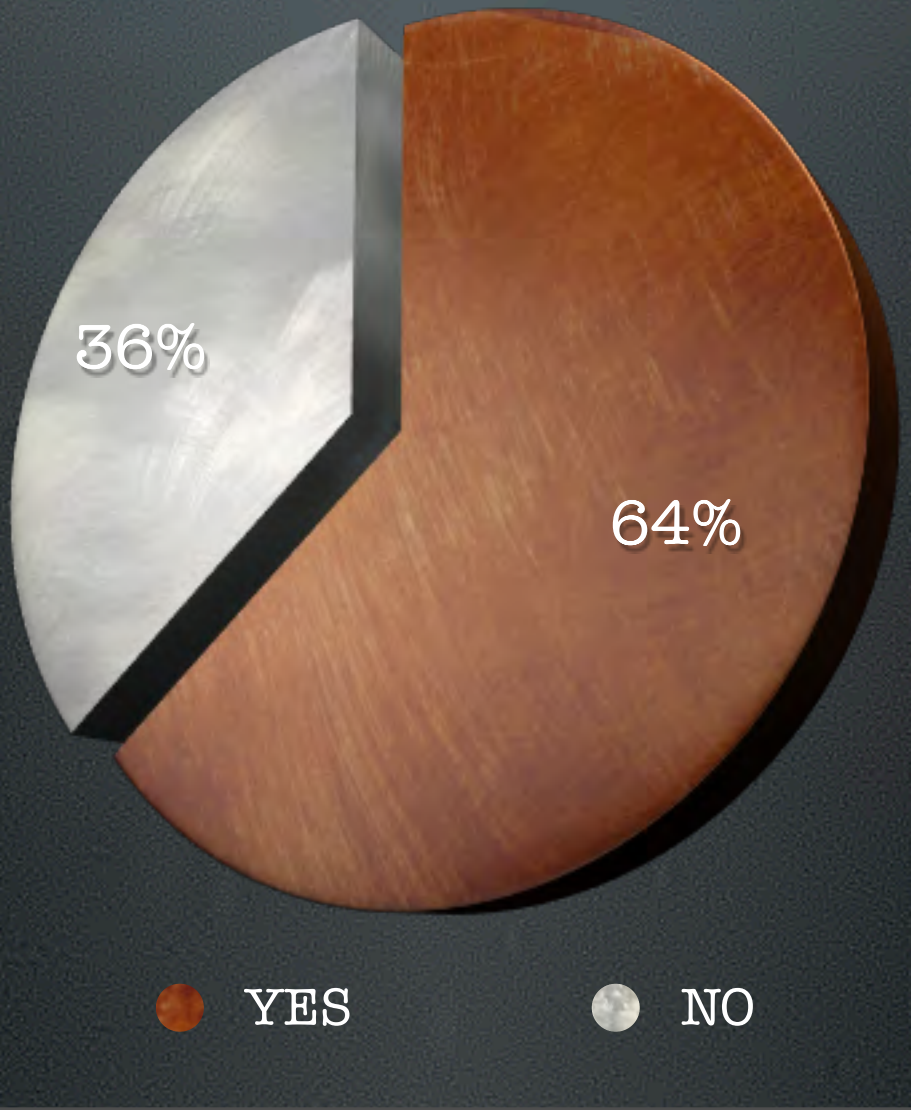
Text

- Different Policies based on Need and Risk
- Different Policies for different users

What Do IACA Members Do?

Closer to Home

Does your jurisdiction have policies regarding the use of personal devices at the office such as personal laptops or smartphones?



IACA Member Policies

	Responses
No personal devices allowed whatsoever	4
Limit the types of devices and applications	3
Personal devices allowed only with a “compelling reason”	1
Preauthorization required	1
VPN Access to internal resources	1
Only allow personal devices to be used during personal time	5
Personal devices allowed but must meet security policies such as having anti-virus installed	1
Wifi is only available to IT staff	1
Guest wifi is only available in public spaces	1

IACA Policy

- Most Deal with Onboarding
- Most are concerned with loss of productivity

Jurisdiction Examples

MONTANA

- Some staff issued smartphones and managed through central device management
- Personal devices that want to use Outlook Web Services must be placed on that policy
- Otherwise, personal devices not allowed on the secure network at all, only a guest network

Jurisdiction Examples

Colorado

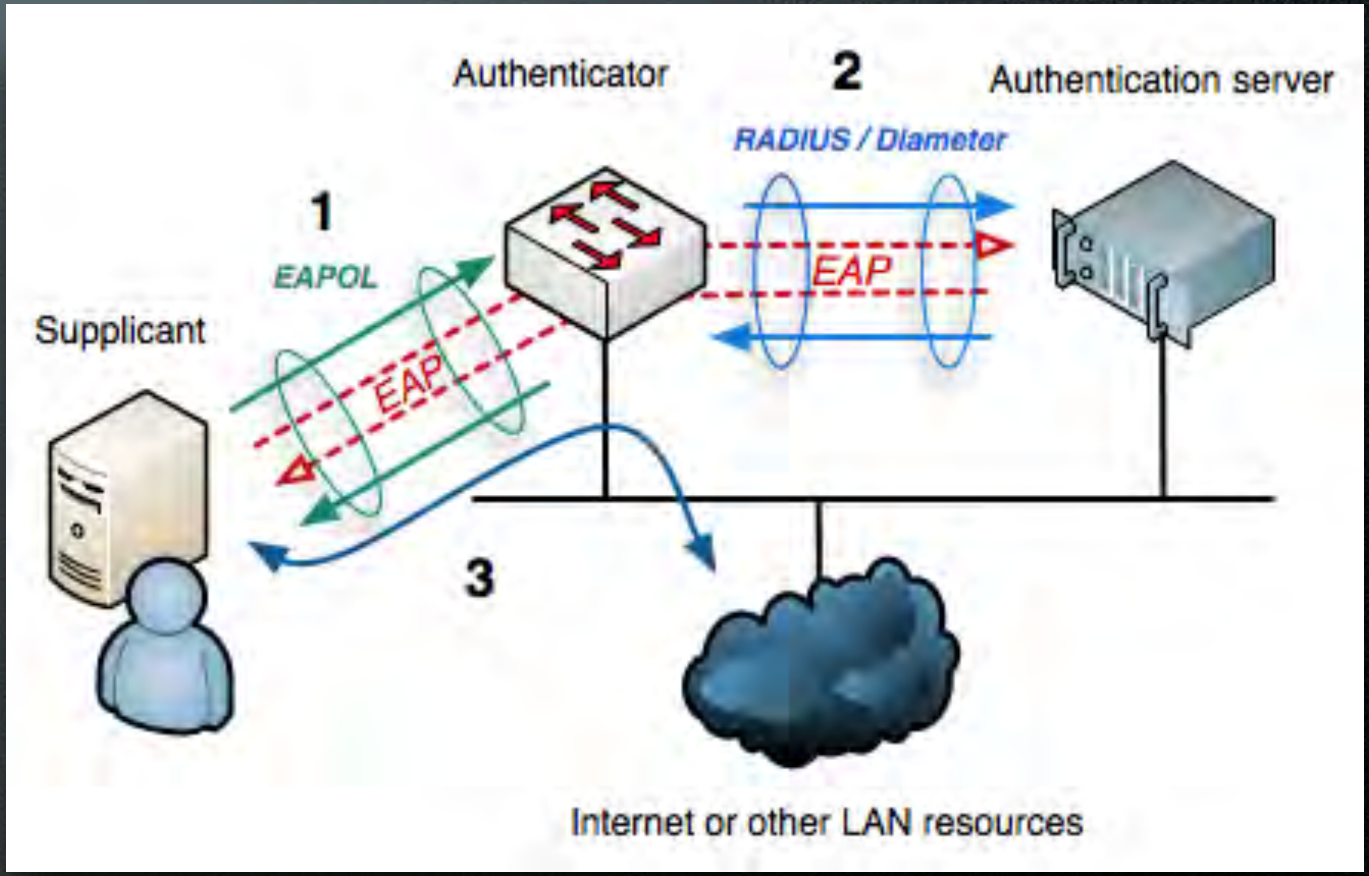
- Internally:
  - Embraced BYOD with limited capabilities (ActiveSync access to iOS, Android, and Windows Mobile for email/calendar/contacts
  - Created policies to address usage and security concerns
  - Created guidelines for evaluating deployment of tablets
- Externally:
  - Focus on mobile browser optimized versions of existing web apps
  - Less focus on native phone applications

Access Control Policy

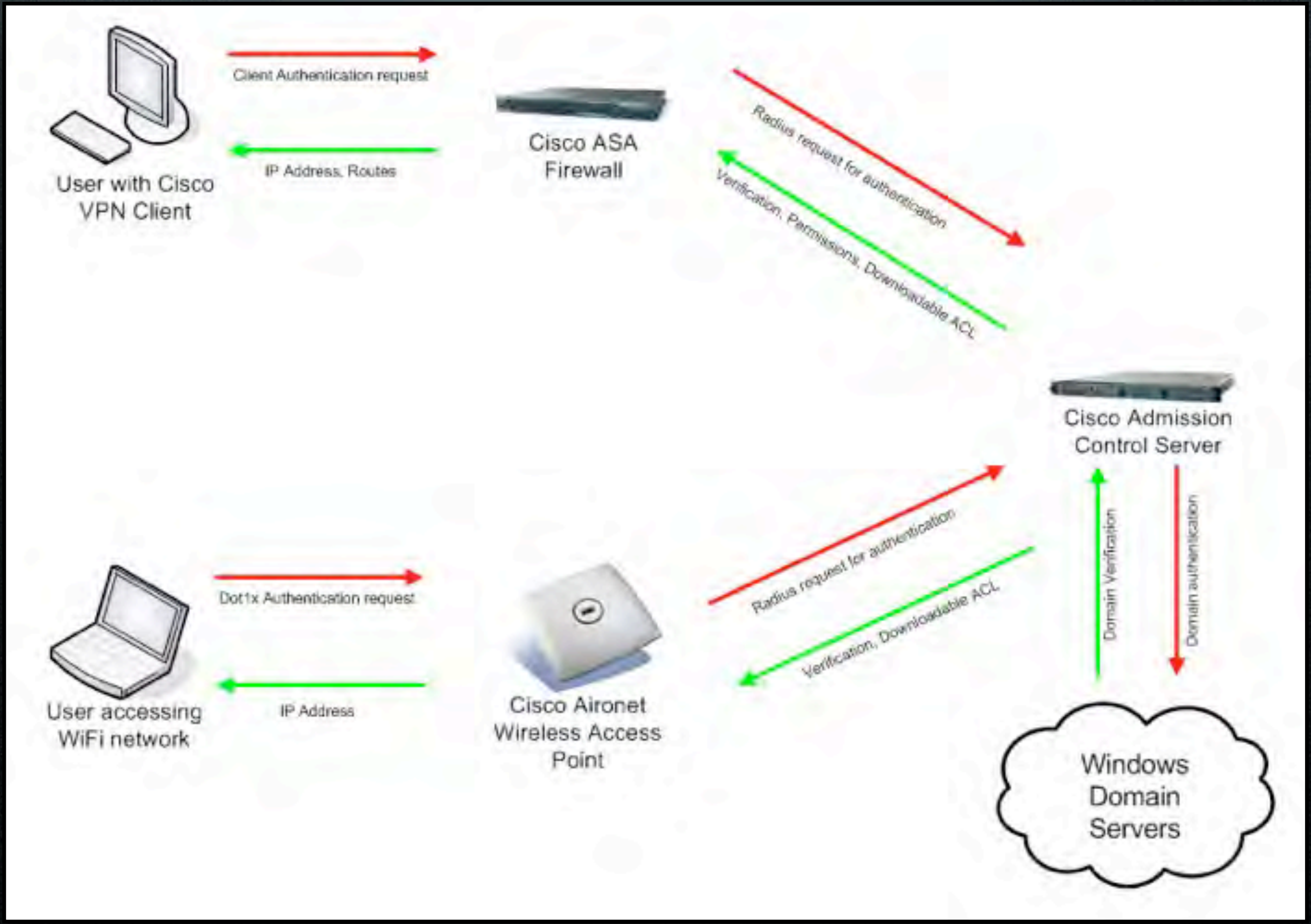
- Limit available network resources
- Control who can access what resources and when access is granted
- Ensure that information remains secure and confidential
- Consider that with an appropriate GENERAL access control policy in place, BYOD is less risky

How Georgia Onboards

What is 802.1x?



Georgia Onboarding


User with Cisco VPN Client
Client Authentication request
IP Address, Routes
Cisco ASA Firewall
Radius request for authentication
Verification, Permissions, Downloadable ACL
Cisco Admission Control Server
Domain Verification
Domain authentication
Windows Domain Servers
User accessing WiFi network
Dot1x Authentication request
IP Address
Cisco Aironet Wireless Access Point
Radius request for authentication
Verification, Downloadable ACL

MDM?

What can MDM Do?

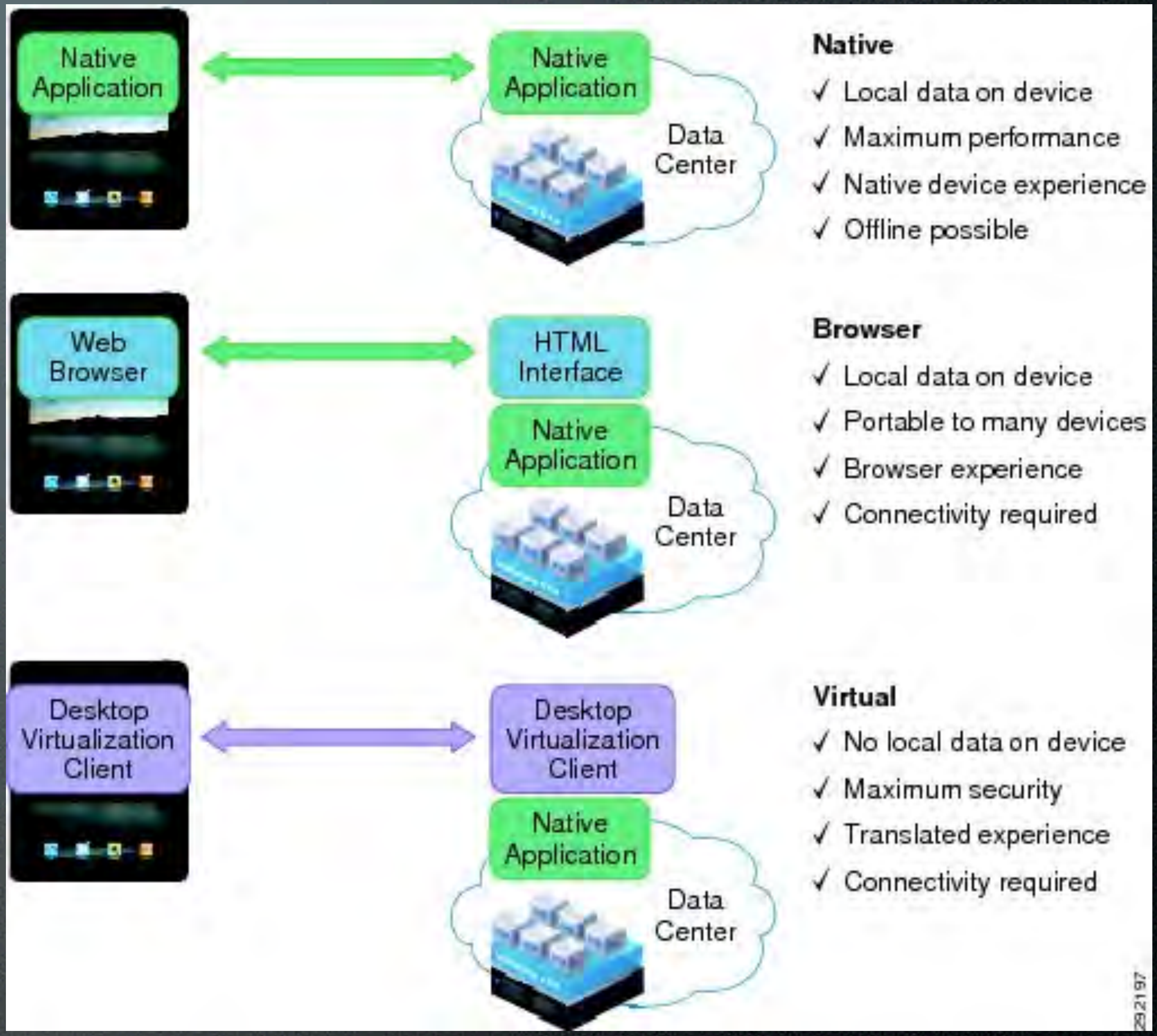
- Password policy, management and enforcement
- Data Partitioning
- Remote application loading
- Remote data wiping
- Whitelist / blacklist apps
- GPS Tracking
- Logging
- Backup/Restore
- More...

MDM Providers

- MobileIron
- ATT Toggle
- MobiControl
- MikiMobility
- Trend Micro mobility

Application Security

- Native Applications
- Browser Based Applications
- VDI



Native

- ✓ Local data on device
- ✓ Maximum performance
- ✓ Native device experience
- ✓ Offline possible

Browser

- ✓ Local data on device
- ✓ Portable to many devices
- ✓ Browser experience
- ✓ Connectivity required

Virtual

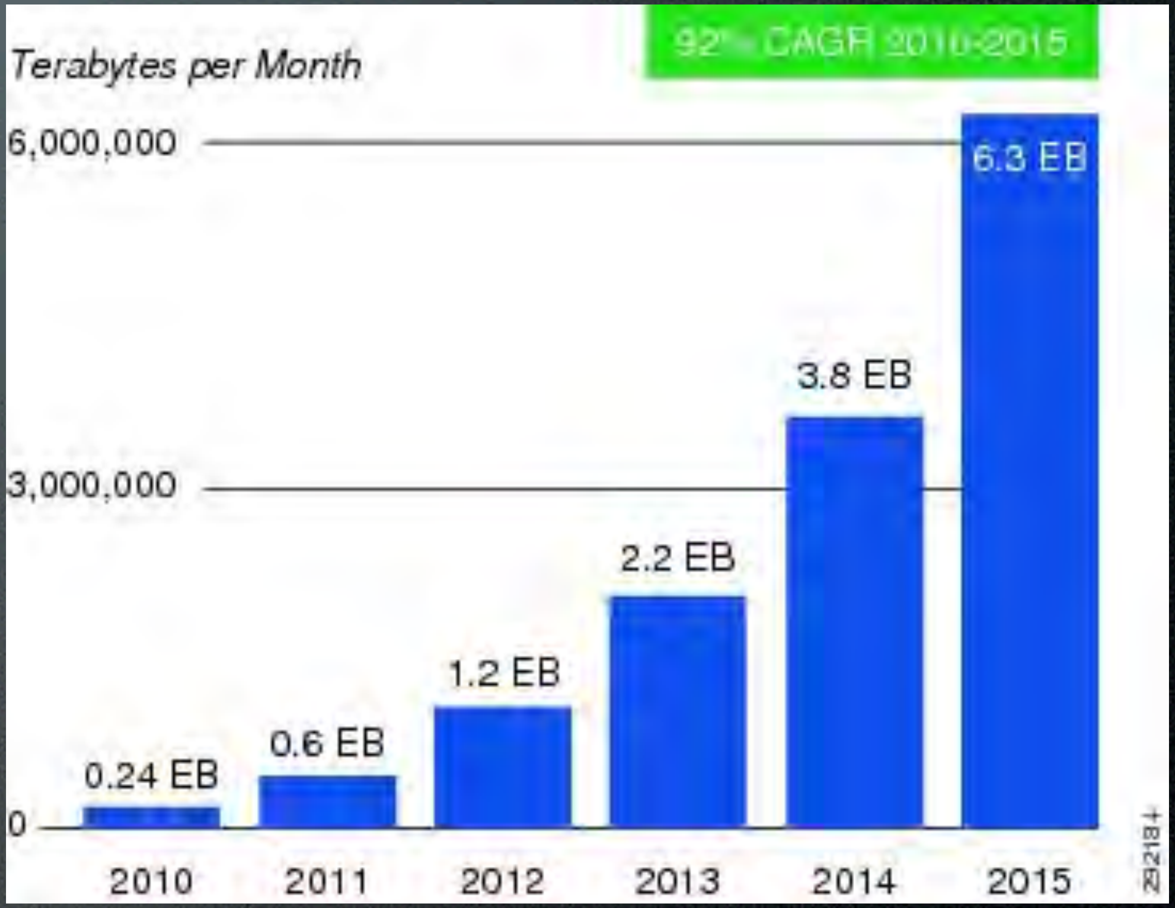
- ✓ No local data on device
- ✓ Maximum security
- ✓ Translated experience
- ✓ Connectivity required

Infrastructure

- Important to realize that wifi is one of the major enabling technologies
- Wifi was originally provided as a mere convenience, but is becoming a primary form of connectivity.
- Limited air space and channels
- Not only is wifi used more often, HOW it is used has changed significantly

Wifi Considerations

- Upgrade to latest standards (802.11n)
- Router should support 802.1x
- Consider a device that has built in QOS



Questions?