Technology Leadership Discussion Series

Bring Your Own Device

October, 2012
Bring Your Own Device (BYOD):
Best Practices for Enabling a Mobile Workforce
Advanced Network Systems

ABOUT US

Established in 1996
25 - Engineering/ Operations/ Sales
Richmond
Charlottesville
Shenandoah Valley
Bluefield
Roanoke Valley

OUR APPROACH

Client-focused
Business-minded
Service/Accountability
Strategic Thinking
Return on Investment

PARTNERSHIPS

WatchGuard
Meru
Microsoft
Vmware
Shoretel
And more. . .
Advanced Network Systems

OUR EXPERTISE

Technologies

- Wireless
- Network Security
- Infrastructure-Virtual Servers & Desktops
- Business Phone Systems
- Network Management (Managed IT)
- Network-Based Video Surveillance
- Videoconferencing

Services

- Technical Services
- Strategic Planning Services
- Implementation Services
- Managed IT Services
- Support Services
- Education Services
What Is BYOD?

**Bring Your Own Device**

- Where computer end-users (Employees/Students) use their personal devices to interface with and access network resources.
- Any Device/Anywhere
- On Gartner’s “Top 10” list of the most significant emerging trends that will impact data centers and information technology from now into the next five years.
- Key to success is figuring out how to empower users of personal devices with network access without compromising security, overwhelming the network and IT staff.
How Big Is BYOD?

It’s bigger than most IT Managers think . . . and growing

Figure 1: Devices used to access business applications

% of employees using smart mobile devices for business use

Q1 (2011), Q4 (2010). When, if any, of the following devices do you use to access your organization’s business applications such as employee benefits, customer billing, client relationship tools, or productivity tools such as spreadsheets, word processors, etc.? 

% of employees using smart mobile devices for business use

Source: IDC information worker custom survey, sponsored by Unisys, May 2011
Q3 (Worker survey). Please indicate whether you use the following devices for PERSONAL activities, BUSINESS activities, or not at all? Q1A (business survey). Approximately what percent of your organization's employees use the following devices for business applications today?
How Big is BYOD?

♦ An Aberdeen study in July 2011 found 75% of organizations are permitting some form of BYOD for business purposes. This is expected to grow to 90% by 2014.

♦ A recent Gartner report found that only 43% of organizations have a formal BYOD policy, with specific rules.
What’s Driving BYOD?

♦ The Proliferation of Consumer Devices
“Consumerization” of IT

In 2012 the number of smartphones will significantly outpace the number of all PCs sold.
Work Life Overlaps with Personal Life

56% of US information workers* spend time working outside the office. —Forrester

*employees who use a PC or mobile device for work an hour or more per day

With busy lives and multiple computing devices, information workers report mixing work and personal use on 60% of the devices they use. Only 14% of devices are used strictly for work and 26% are purely personal use.
What’s Driving BYOD?

♦ The Expectation of Anywhere, Anytime Mobility

Worldwide Mobile Data Forecast 2010-2015

Source: IDC 2011

![Bar chart showing terabytes per month for mobile data forecast from 2010 to 2015](chart.png)

- 2010: 0.24 EB
- 2011: 0.6 EB
- 2012: 1.2 EB
- 2013: 2.2 EB
- 2014: 3.8 EB
- 2015: 6.3 EB

92% CAGR 2010-2015
What’s Driving BYOD?

♦ Applications!!!! Huge amount of Availability and Growth
♦ Collaboration
♦ Digital Interactive Media
♦ Video
Why Employees Like BYOD

♦ 41% of people in the US already carry a smartphone with them today!
♦ Employees want the flexibility to perform personal activities at work, and work activities during personal time.
♦ Employees increasingly have access to better technology in their personal life than their professional life!
♦ Work (and the worker) is increasingly mobile, distributed and collaborative.
♦ Younger employees (and future employees) are already tech-savvy, mobile, and cloud-based — feel they are more productive on devices they know
Why Companies Like BYOD

♦ Improves employee productivity
  — more opportunities to collaborate
  — easier to get work done using technology they like & are comfortable with

♦ Employers who enable choice and flexibility in the workplace demonstrate a greater sense of job satisfaction.

♦ The cost savings benefits of BYOD (device and/or service) vary based on employer policy, employee’s position and work requirements.

  IBSG estimates that the annual benefits from BYOD range from $300 to $1,300 depending on the employee’s job role.
BYOD Benefits: A Two-Way Street

♦ Most organizations believe their employees work more hours as a result of this accessibility.

♦ Employees appreciate and welcome the enhanced work-life balance that comes when employees have more freedom and choice to get work done whenever and wherever they need to — whether that's in the office, on the road or while sitting in the stands at a child's baseball game.
Support of BYOD by Industry

Which Organizations are Embracing BYOD?

[Bar chart showing the percentage of organizations currently supporting or planning to support BYOD in different industries.]
Almost all K-12 and higher education institutions have some type of BYOD policy.

Education LOVES BYOD because:

- Students already have devices or access to a device
- Helps K-12 achieve one-to-one computing
- Provides technology access without financial burden
- IT doesn’t have to be involved in device support
- Schools can shift toward more digital content
- Engages students boosts academic achievement (technology is the great equalizer)

BYOD helps bridge the gap.
BYOD Is Here To Stay

- IT Depts are being forced to deal with an influx of end-user devices—whether they like the concept or not.
- BYOD is more than just shifting ownership of the device to the end-user. It has complex implications for companies and their IT departments.
- A strategy needs to be defined in advance of implementation.
BYOD Implementation Challenges for IT

♦ Providing Device Choice and Support for All Devices
♦ Maintaining Secure Access to the Network
♦ On-Boarding of New Devices
♦ Visibility of Devices on the Network
♦ Managing the Increase in Connected Devices
♦ Ensuring Wireless LAN Performance and Reliability
♦ Enforcing Company Usage Policies
♦ Protecting Data, Loss Prevention and Revoking Access
BYOD Strategy Options

♦ Understand User Segments and Needs
♦ Who Really Benefits from BYOD?
BYOD Strategy Options

Deciding on a BYOD Adoption Strategy
BYOD Strategy Options

♦ Considering Application Strategies
  Consumable (web-based/read-only)
  Production (applications)

♦ Extending Collaboration to BYOD Devices

♦ Have an Encompassing End User Agreement

♦ Have a Lost or Stolen Policy
KEYS TO BYOD SUCCESS

- Infrastructure
- Policy
- Operations / Support
- Security
BYOD: A Network Perspective
BACKGROUND ON MERU NETWORKS

• Founded in 2002, Sunnyvale, CA, USA
  – Operations in North America, APAC, EMEA
• NASDAQ Listed – “MERU”
• Vision: The All-Wireless Enterprise™

  Network in Control Client Access
  through Virtualized Wireless LAN innovation

• 6,500+ customers in 55 countries worldwide
• Patents in several wireless technologies
  – Radio frequency management
  – Switched wireless architectures
  – Wireless service assurance
  – Proactive diagnostics and management
  – Optimized application performance
The Meru Portfolio

- Centralized Management
- Identity Management
- Security Services
- Service Assurance

Meru System Director

| Small Office / Remote Location | Branch Office 1-5 AP’s | Regional Office 50-100 AP’s | HQ / Central Campus Indoor / Outdoor 100-1,000 AP’s | Distributed Enterprise 1,000+ AP’s |
POLL

Which IT Challenge is most relevant to you?

a. Network scale
b. Network resiliency and redundancy
c. Reliable application delivery and integrity
d. Secure Guest and User access
What are the ramifications of BYOD on your network infrastructure?

Out of scope:
- App development
- Device and service liability
- Carriers or 3G/4G
GAME CHANGER

Launched Mar’10

100M units by 2012*

25% of guest traffic on hotel networks from Apple iOS**

All have Wi-Fi, but lack an Ethernet port

Ideal for Video Consumption

Average hotel Internet Session has grown 5MB ⇒ 15MB from ‘09-’11**

*Gartner Group

**iBAHN
THEY’RE COMING!

• 1.9 Billion Wi-Fi devices hitting the network by 2014*
• Up to 67% are BYOD
• 25-50%/year churn assuming 18mo-3yr cycle
• Expected Benefits
  – Up to 30min/day productivity**
  – Lower device capex

*Source: In-Stat  **Source: Aberdeen
BYOD EXAMPLES ACROSS INDUSTRIES

Some budget conscious schools may view BYOD as a 1:1 laptop alternative.

Customer engagement is better on shopper’s own smartphones and tablets, and it’s more cost effective.

On a college campus, most every device is BYOD – especially after Christmas!

Physicians often bring their own devices for rounds, while patients and their families use Wi-Fi to research medical conditions.
THE TROUBLE WITH TABLETS

Without Proper Planning, Enterprises Deploying iPads Will Need 300% More Wi-Fi

Published: 21 October 2011

Gartner Research
Analyst(s): Tim Zimmerman

*iBAHN comparison to laptops*
IT Network Infrastructure Challenges

Client Provisioning

- Wireless Network
- Security Profile
- Quality-of-Service

Network Provisioning

- Traffic Separation
- Access Control

Performance

- Scale
- Roaming
- Over-the-air QoS
- Interference

How do I…

- “make sure the RF spectrum is clear?”
- “migrate from 5% wireless to 50% wireless?”
- “scale the network, not the IT team?”
Wi-Fi Meltdown

Wi-Fi Overload at High-Tech Meetings

*NY Times, Dec 28, 2010*
Why does this happen?

Because the clients are in control:
- Clients decide when to transmit
- Clients decide which radio to use
- Clients decide when to roam
- Clients decide whether to use QoS
- Clients only use the security they are configured for…
SOLUTION

What if... put the network-in-control of client access?

... simplifies provisioning and deployment
... automatically provisions 802.1x for users
... picks best channel and AP for client
... picks who can transmit, and for how long
... provides flawless voice & video
... enables zero-handoff roaming
... uses proactive network management for service assurance
## BYOD Solution Components

<table>
<thead>
<tr>
<th>Identity Management</th>
<th>Device Management</th>
<th>Device Provisioning</th>
<th>Spectrum Management</th>
<th>Service Assurance Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Users</td>
<td>• Device encryption</td>
<td>• Wireless profiles</td>
<td>• Rogues</td>
<td>• Proactive network verification</td>
</tr>
<tr>
<td>• Devices</td>
<td>• Lock-out</td>
<td>• Agents, etc</td>
<td>• Non-802.11 Interferers</td>
<td>• Station history and diagnostics</td>
</tr>
<tr>
<td>• Guests</td>
<td>• Upgrades, etc</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Network Infrastructure Control

- **Authentication**
  - Encryption
- **Access Control**
  - Roaming
- **Load-balance**
  - Call Admission Control

![Device Images](Android, iPhone, Windows Phone)
BYOD Solution Topology

Identity Manager

Device Manager

Generic application services

User Repository (AD)

Spectrum Manager

WLAN Controller

Enforcement Point

Wi-Fi Aps and sensors

Wi-Fi mobile workstations, smartphones, and tablets

Netbook/notebook

iPhone

iPad

Android

Windows Phone

Device Provisioning (all OS)
# LIFE WITH ‘NETWORK-IN-CONTROL’

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>K-12</td>
<td>1:1 Laptop login for 30 laptops in 90 seconds instead of 10 minutes</td>
</tr>
<tr>
<td>Finance</td>
<td>1,200 users in trading pit with uSec SLAs</td>
</tr>
<tr>
<td>Wholesale</td>
<td>FMC on iPhones with fast voice roaming on palette movers</td>
</tr>
<tr>
<td>Higher Ed</td>
<td>½ FTE managing WLAN campus coverage for 60 buildings, 2 million sq ft</td>
</tr>
<tr>
<td>Enterprise</td>
<td>10,000 devices securely provisioned automatically with 802.1x</td>
</tr>
</tbody>
</table>
Key Takeaways

• If you deployed a state-of-the-art WLAN before April 2010, it’s time to re-assess your needs.
• You have to take into account capacity and reliable application delivery as well as security.
• You need to take control from the client, and put control back into the network.
About WatchGuard

- Founded in 1996 – privately held
- Firewall appliance pioneer
- HQ in Seattle, WA, 600+ employees globally
- 100% channel – 15,000 partners in 120 countries
Who Relies on WatchGuard

Government
- National Defence
- Government of Canada Privacy Council Office
- City of Vancouver
- Government of Canada

Finance & Insurance
- Banco Popular
- ING
- Diback Austria
- Alliance Trust
- Farmers Credit
- Credit.com
- Mayo Clinic
- Mayo Clinic

Healthcare
- Baxter
- Anglophone Blood Center
- Heart & Stroke Foundation
- Imperial Health Care
- NHS
- Samsung
- Danaher
- GRH
- Trek

Manufacturing
- Mitsubishi Electric
- Eaton
- Danaher
- Samsung
- Siemens
- Netgear

Technology
- IBM
- Toshiba
- Raytheon
- Unisys
- Netgear

Entertainment
- Univision
- Marriott
- Cinemagic

Retail, Food, & Services
- IKEA
- Marriott
- Sheetz
- RWE
- Ravensburger

Telecom & ISP
- Telus
- Etisalat
- Paetec
- Marinix

Education
- Penn
- Long Island Rail Road
- Washburn University

Automotive & Transportation
- Toyota
- Western Airlines
- Animal Humane Society

Non-Profit
- The Salvation Army
Security concerns are the #1 inhibitor to BYOD adoption!

Loss of Control!

what’s wrong with byod?

No Control = No Security
Recent mobile Threats

- Symbian & BB malware helps Zeus steal pwds
- Malware explodes on Android Marketplace
- First wild Android drive-by download
Two 2012 Mobile Predictions:

1. **BYOD means clean your own infection**
   - BYOD adoption will result in **more data loss** during 2012

2. **Digital weeds in mobile App gardens**
   - Mobile threats will primarily propagate via **infected App stores**

**Loss of Control!**

- Open gardens repeatedly hit with malware
- Walled-gardens aren’t safe either
General Mobile Device Tips

• Creation of IT acceptable use policy – Mobile Devices
• Enforce lock screen and/or password
• Encryption and VPN
• Consider mobile security software
• Be careful of what you download
BYOD Tips

• Acceptable Use Policy – Section specific for BYOD
• Built in Security (example: Active Sync)
• Mobile Device Management (MDM)
• Virtual Desktops
BYOD/Firewall Practices to Consider

- Wi-Fi network specifically for BYOD Devices
  - Unique Subnet
  - Unique DHCP scope
  - Enforce User Authentication

- Advantages for implementing (the above)
  - Enforce Firewall Policies that segments these devices from other corporate resources
  - Enables firewall policy enforcement via username and/or group
  - Positively identifies a user and associates user to a device
  - Audit Trail / Logging
  - Enables visibility of user/device usage in reports
Trick plays may win the BYOD security game once in a blue moon. Firewalls that offer Fundamental Security features will win more often!
BYOD Summary

♦ Evaluate Organizational Requirements
  Who could benefit?
  Are people already implementing it?
♦ Adopt a Strategy, Policies, Procedures
♦ Prepare Your Infrastructure
♦ Build in Security at Every Opportunity
♦ Roll Out a Complete Service
  Test drive before full implementation
♦ Evaluate and Adjust
Questions?

YOUR PRESENTER:
Tony Petrella
800.639.6757
tpetrella@getadvanced.net
www.getadvanced.net