BYOD – Business year of decision!
Cisco on Cisco

Christoph Nienhaus
IT Leader for EMEAR Central - DACH
BYOD – Simpler than you think...
Trendsetter

The Conservative

Don’t worry be happy!
110 million subscribers in the USA.
43.4 million subscribers in the UK.
85.2 million subscribers in China.
3.5 million subscribers in India.
720 million subscribers in total.

2000

323 million subscribers in the USA
59 million subscribers in the UK
963 million subscribers in China
884 million subscribers in India
5.9 billion subscribers worldwide

2011
There Are More Mobile Phones Than Toothbrushes (5B vs 2.2B)
Cisco’s Any Device Landscape (Mar. 31, 2013)

Corporate Laptops (CYOD)
- Windows: 84,696
- Linux: 7,264
- Apple: 33,780

Corporate VXI Endpoints
- Other: 3,101

Mobile Devices (BYOD)
- Apple: 15,873
- Android: 32,536
- Other: 5,401
- BlackBerry: 806

Growth Rates:
- Corporate Laptops: 4.4% Growth
- Corporate VXI Endpoints: 3.8% Growth
- Mobile Devices: 11.7% Growth
- BlackBerry: -11.5% Growth
- Other: 0.3% Growth
Mobile Device Share

**Android**
- Has achieved a 3 month avg. growth high of 11.7%
- March share up from 12% in 2012 and 7% in 2011

**iOS**
- The most popular combination of devices is the iPhone + iPad, with 10,685 users having this combination

**BlackBerry**
- The 8% share is a significant fall from the same period in 2012 of 22% and 41% in 2011

Source Data: ISA Server Stats via Adam Grimes – adgrimes@cisco.com, EMAN Mobile Admin
BYOD or The Post PC Era
or “Getting back the control…”
Device
- Smart-Phone \ Tablet
- Virtual \ Laptop
  - VIRTUAL Clients
  - Desktop\Notebooks

Application
- Cisco Owned APPS
  - Platform
  - Web
- Personally Owned APPS

Data
- Corporate
  - Multiple Locations
- Personal
- PC Backup

Device Security
- Encryption
  - Windows
  - Macs
- Anti-Virus
  - Windows
  - Macs
- Behaviour-Analytics

Network Security
- IRON-PORT \ WSA (SECURITY APPLIANCE)

Network
- ANY-CONNECT
- CORPORATE
- GUESTNET
- PUBLIC

Device Management
- Non-Standard
  - Windows Altiris
  - Mac to be decided
  - Mobile Afaria

App Delivery
- Disparate
  - Point Solutions
  - App Centre
  - Soft-Tracker
  - Image - ACNS

Device Provisioning
- Multi-Source
  - Global Desktop Management
  - Service Catalogue
  - MDS Mobile
Challenges & Opportunities

How to evolve our technologies and policies to cater for new devices, operating systems, form factors and ownership

For example one of the growing challenges is protecting our data. This could be done with a number of technologies in the future such as:

- Web apps e.g. Microsoft Web Apps
- Containerisation e.g. Good or Touchdown
- Virtualisation (local or remote, application or full desktop) e.g. Citrix, VMware, Microsoft
- Digital Rights Management (DRM) e.g. Microsoft

We currently rely on a culture of trust to support security policy …. we may need to adjust the balance to protect our data in the Post PC world
Architecture Future State (FY16) – User Focus

Identity & Context
- Who
- Role: HR
- Where
- When
- How
- Policy

Policy / Entitlement
What applications can you access?

Context Compliance

Device ID
What devices can you use?

UserID

Device Management

Devices, Appliances & Things

Public/Private Cloud

Cisco Enterprise Store

WebEx

Social Files

Compliance
Policy / Entitlement

Trusted / Untrusted

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy

Who
- Role: HR
- Where
- When
- How
- Policy
The Four Stages of Secure BYOD

**Profiling**
- **User Impact**: Entirely transparent to users
- **IT Impact**: Creation of a live "endpoint database"
- **Value**: Visibility into device & user demographics
  - Ability to make informed business & security decisions

**Registration**
- **User Impact**: Users register their devices for corporate access. Network configures BYOD devices for users. Guests use internet.cisco.com SSID is "internet" ("guestnet" retired)
- **IT Impact**: New guest/BYOD network BYOD onboarding
- **Value**: Foundation for unique device identifier for device management.
  - Streamlined onboarding (reduced support costs)

**Posture**
- **User Impact**: Corporate & BYOD devices have posture assessed
- **IT Impact**: Deployment of Mobile Device Management (MDM) client on endpoints
- **Value**: Visibility into security posture
  - “How many jailbroken iPhones are being used on our network?”
  - “Who has disabled PIN and screensaver on their device?”

**Enforcement**
- **User Impact**: Access to corporate network governed by “context”, including identity, role, device, posture etc
- **IT Impact**: Creation of a live "endpoint database"
- **Value**: Fine grained policy based network access model
  - Differentiated/virtualized access based on context
  - Security no longer based on perimeter

*(capabilities mature over time)*
Mobile Device Security Model
Current State

Other Devices

- 10 Minute Timeout
- 4 Digit PIN

Trusted Devices

- Local and Remote Wipe
- Encryption and Management
Mobile Device Access Model

Current State

Network Edge

Other Devices

Remote Wipe

4 Digit PIN

10 Minute Timeout

Encryption

Management

Core Network

Trusted Devices
All users must accept rules of use when signing up for service.

There is no IT jargon – the rules are simple for end-users to understand.

Cisco has a trade off between employee trust and IT control.

**Cisco Rules of Use**

1) Allows Cisco to remotely wipe the device
2) Requires an acceptable password and 10 minute timeout
3) Requires users to immediately report a lost or stolen device.
Employee Education & Responsibility
Code of Business Conduct

HR policy

Signed yearly by every employee

Added the following section to cover personal devices:

“Cisco has the right to require security controls on all electronic and computing devices used to conduct Cisco business or interact with internal networks and business systems, whether owned or leased by Cisco, the employee or a third party. **Cisco also has the right to inspect at any time, all messages, files, data, software, or other information stored or transmitted on these devices.**”
Execution
Cisco Identity Services Engine (ISE)

Consistent Security Policy Enforcement Network-wide
  Physical desktops, virtual desktops, BYOD
  Wired, Wireless, VPN*
  Bound to point of access, not IP address

Supports Data Security, Access Control, and Compliance
  Protects intellectual property

Automation & Self Registration

Context-aware Identity and Authentication Services

WHO  WHAT  WHERE  WHEN  HOW
Apps, apps, apps and more…
A multitude of “stores” at Cisco
Cisco Enterprise Store

- Access to Storefront from all OS & Device Types
- Pervasive Enterprise Security (versions, enforcement, trusted devices)
- Personalized, User Friendly Catalog for all IT Services
- Integrated with Enterprise Service Management
- Automated and Seamless Service Provisioning

Desktop Apps
- Mobile Apps
- Quad Apps

Virtual HW
- Desktop HW
- Mobile HW

Reporting
- Chargeback
- Entitlement
- Approvals
- Categories
Conclusion
Evolving workplace....

- No ‘automatic’ entitlement to internal network access – registration will be required
- Devices not able to authenticate will have no direct access to internal resources
- Future state is differentiated access based upon device type, state, posture – and user
- “Flat” network access no longer
  - Some vendors forced into ION for VDI only access (data security)
  - Physical loop holes closed where currently exploited
  - “Follow the user’ access control
- Better user experience through leveraging pervasive identity
What have we learned?

Higher user expectations

Products & Capabilities are still maturing

- Users don’t care about certs, MAC addresses, provisioning…
- “Just make it work!”

Bring Your Own Device = Brought Your Own Device

- They’re already here.
- Adapt or pay the price in lower user experience & serious security implications

So many platforms, variations, brands…

- Aim for large targets first
- You’ll never cover every version, brand or flavour of Android (for example)

Community support, workshops and “social networking” works

- Mindset of today’s employees is different
Thank you.