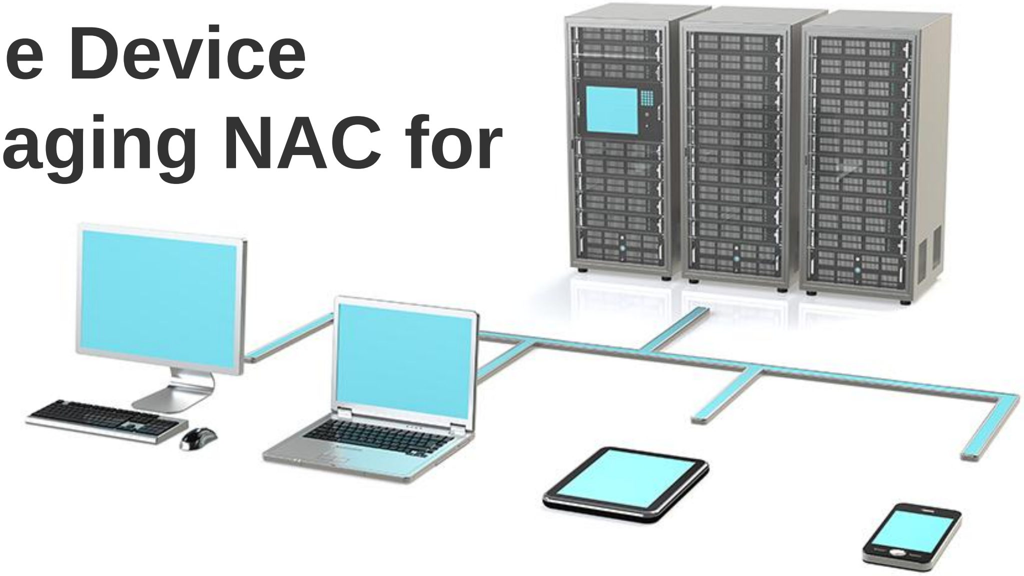
# Going Beyond Mobile Device Management - Leveraging NAC for Mobile Devices



G. Mark Hardy, CISSP, CISM

President, National Security Corporation

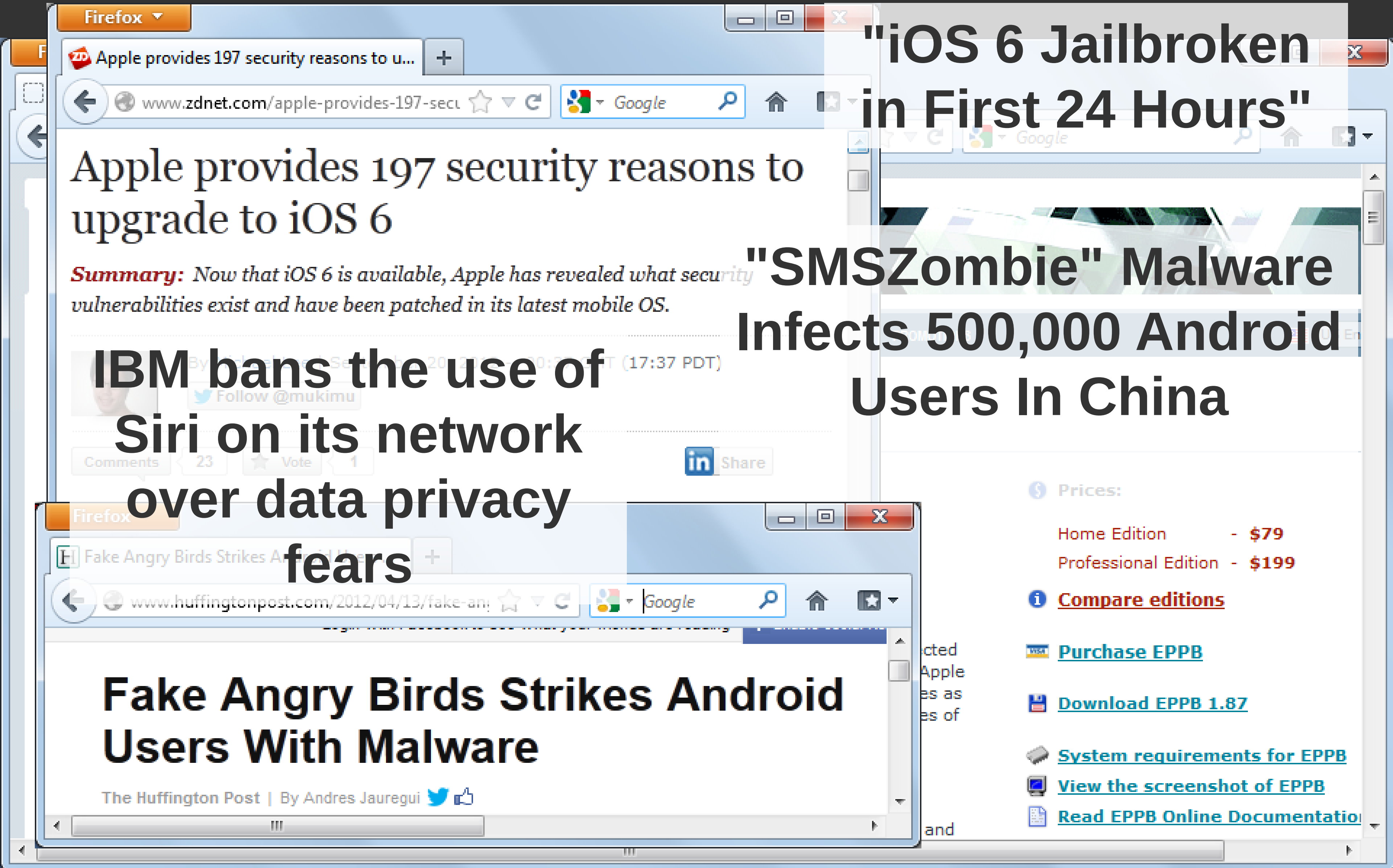
gmhardy@nationalsecurity.com

+1.410.933.9333

# Agenda

- Current state of mobile security
- Mobile device security strategies and resources
- Mobile Device Management (MDM)
- Endpoint Protection Platforms (EPP)
- Governance, risk, and compliance (GRC) and risk management
- Network Access Control (NAC)
- Next-generation technologies
- Future vision

# Mobile Device Security is Hard



"iOS 6 Jailbroken in First 24 Hours"

"SMSZombie" Malware Infects 500,000 Android Users In China

IBM bans the use of Siri on its network over data privacy fears

Firefox
Apple provides 197 security reasons to u...
www.zdnet.com/apple-provides-197-secu
Google

Apple provides 197 security reasons to upgrade to iOS 6

*Summary: Now that iOS 6 is available, Apple has revealed what security vulnerabilities exist and have been patched in its latest mobile OS.*

(17:37 PDT)

Follow @mukimu
Comments 23
Vote 1
in Share
Firefox
Fake Angry Birds Strikes A
www.huffingtonpost.com/2012/04/13/fake-an
Google

Fake Angry Birds Strikes Android Users With Malware

The Huffington Post | By Andres Jauregui

cted Apple es as es of and

Prices:

| | | |
|---|---|---|
| Home Edition | - | $79 |
| Professional Edition | - | $199 |

Compare editions

Purchase EPPB

Download EPPB 1.87

System requirements for EPPB

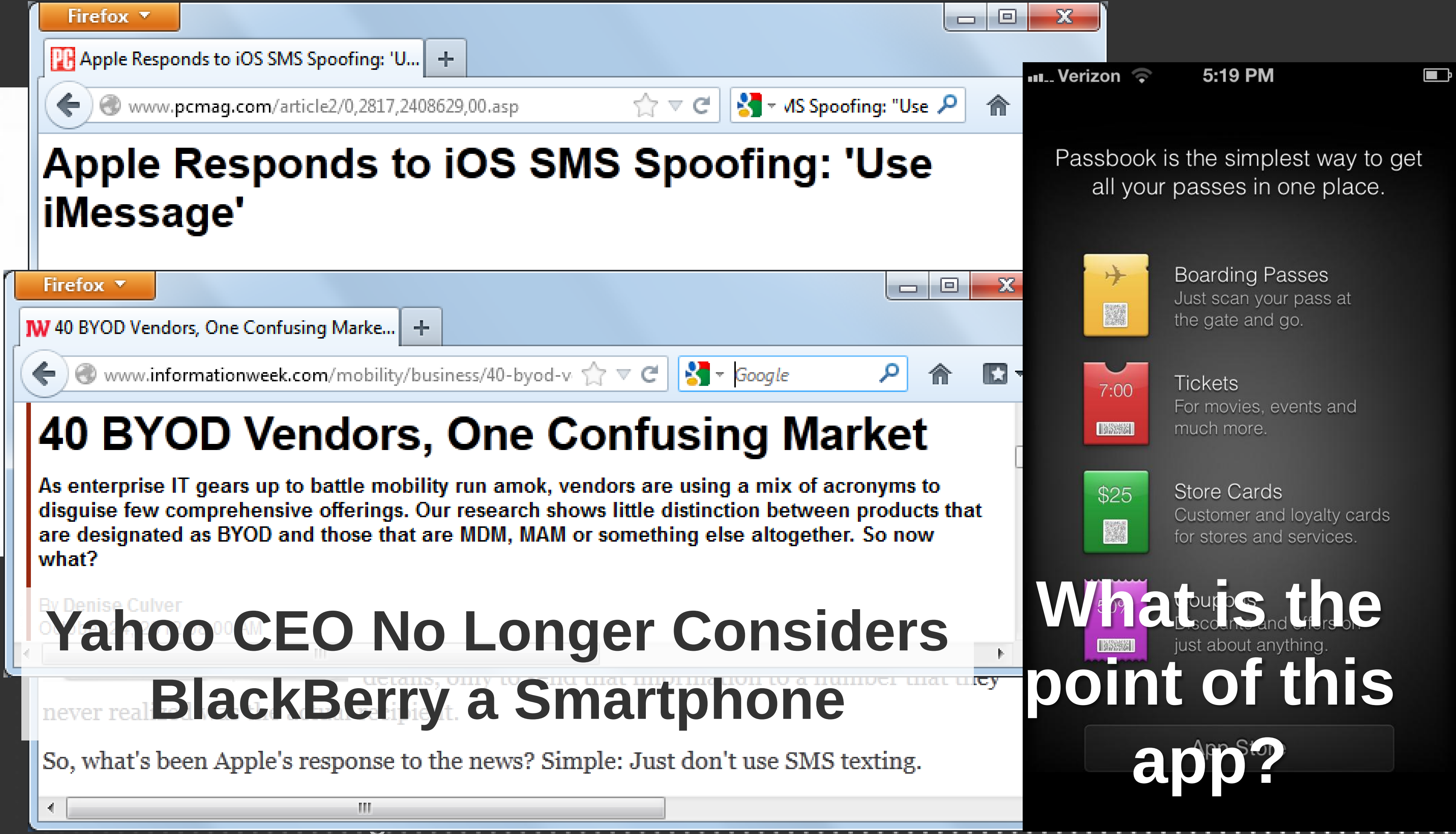
View the screenshot of EPPB

Read EPPB Online Documentatio

With thanks to Chris Crowley/Joshua Wright from SANS

TechTarget

# Mobile Security is Confusing



Firefox
Apple Responds to iOS SMS Spoofing: 'U...
www.pcmag.com/article2/0,2817,2408629,00.asp
MS Spoofing: "Use
Firefox
40 BYOD Vendors, One Confusing Marke...
www.informationweek.com/mobility/business/40-byod-v
Google
Verizon
5:19 PM

Apple Responds to iOS SMS Spoofing: 'Use iMessage'

40 BYOD Vendors, One Confusing Market

As enterprise IT gears up to battle mobility run amok, vendors are using a mix of acronyms to disguise few comprehensive offerings. Our research shows little distinction between products that are designated as BYOD and those that are MDM, MAM or something else altogether. So now what?

By Denise Culver

details, only to send that information to a number that they never realized was the actual recipient.

So, what's been Apple's response to the news? Simple: Just don't use SMS texting.

Passbook is the simplest way to get all your passes in one place.

Boarding Passes
Just scan your pass at the gate and go.

Tickets
For movies, events and much more.

Store Cards
Customer and loyalty cards for stores and services.

Coupons
Discounts and offers on just about anything.

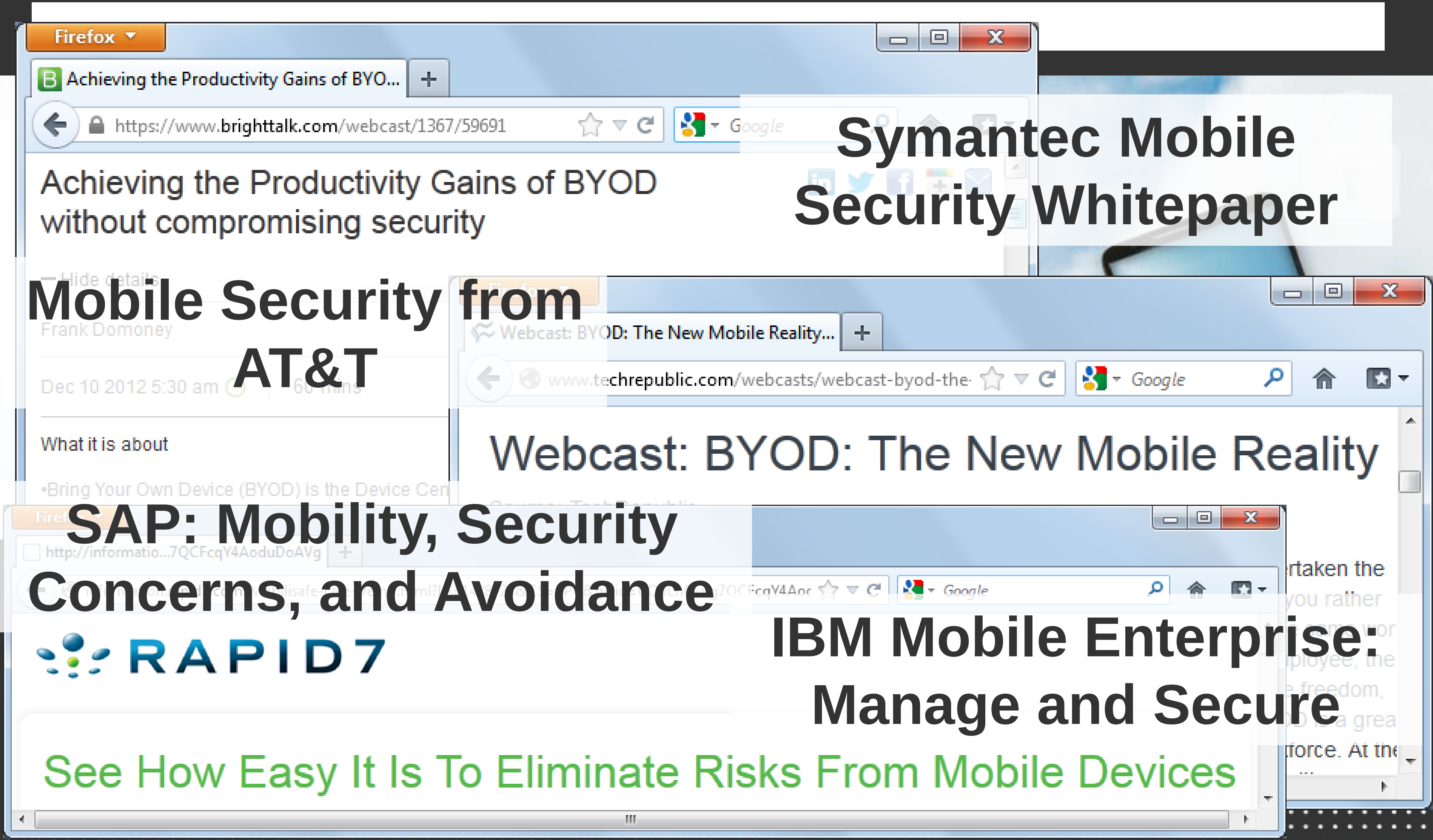
App Store

Yahoo CEO No Longer Considers BlackBerry a Smartphone

What is the point of this app?

With thanks to Chris Crowley/Joshua Wright from SANS

# Vendors All Have Something To Say About Mobile Security


Firefox
Achieving the Productivity Gains of BYO...
https://www.brighttalk.com/webcast/1367/59691
Google
Webcast: BYOD: The New Mobile Reality...
www.techrepublic.com/webcasts/webcast-byod-the-
Google
http://informatio...7QCFcqY4AoduDoAVg
Google

Achieving the Productivity Gains of BYOD without compromising security

— Hide details

Frank Domoney

Dec 10 2012 5:30 am | 60 mins

What it is about

•Bring Your Own Device (BYOD) is the Device Cen

Webcast: BYOD: The New Mobile Reality

rtaken the
you rather
ployee, the
e freedom,
D is a grea
force. At the

RAPID7

See How Easy It Is To Eliminate Risks From Mobile Devices

**Symantec Mobile Security Whitepaper**

**Mobile Security from AT&T**

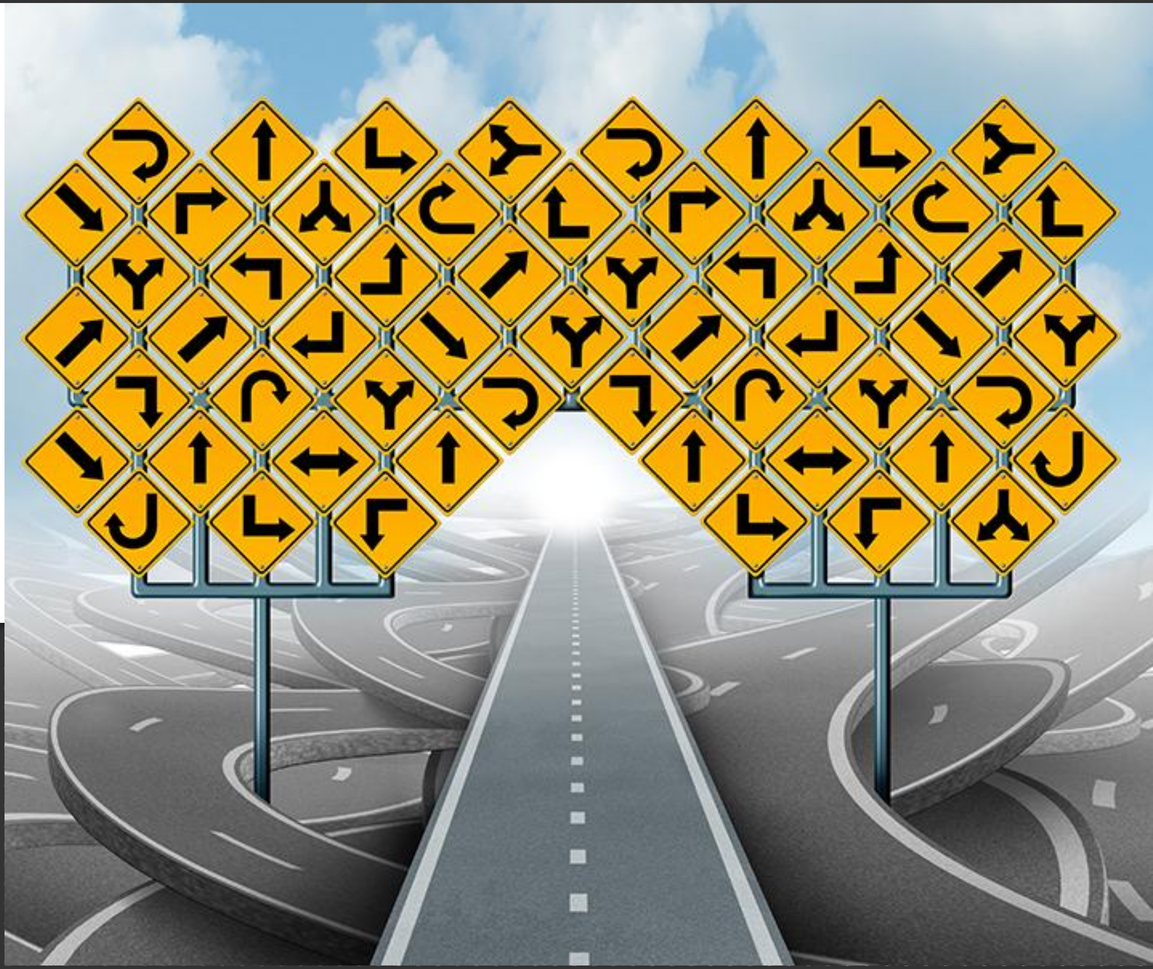
**SAP: Mobility, Security Concerns, and Avoidance**

**IBM Mobile Enterprise: Manage and Secure**

With thanks to Chris Crowley/Joshua Wright from SANS

# Everybody's

# Got An Answer

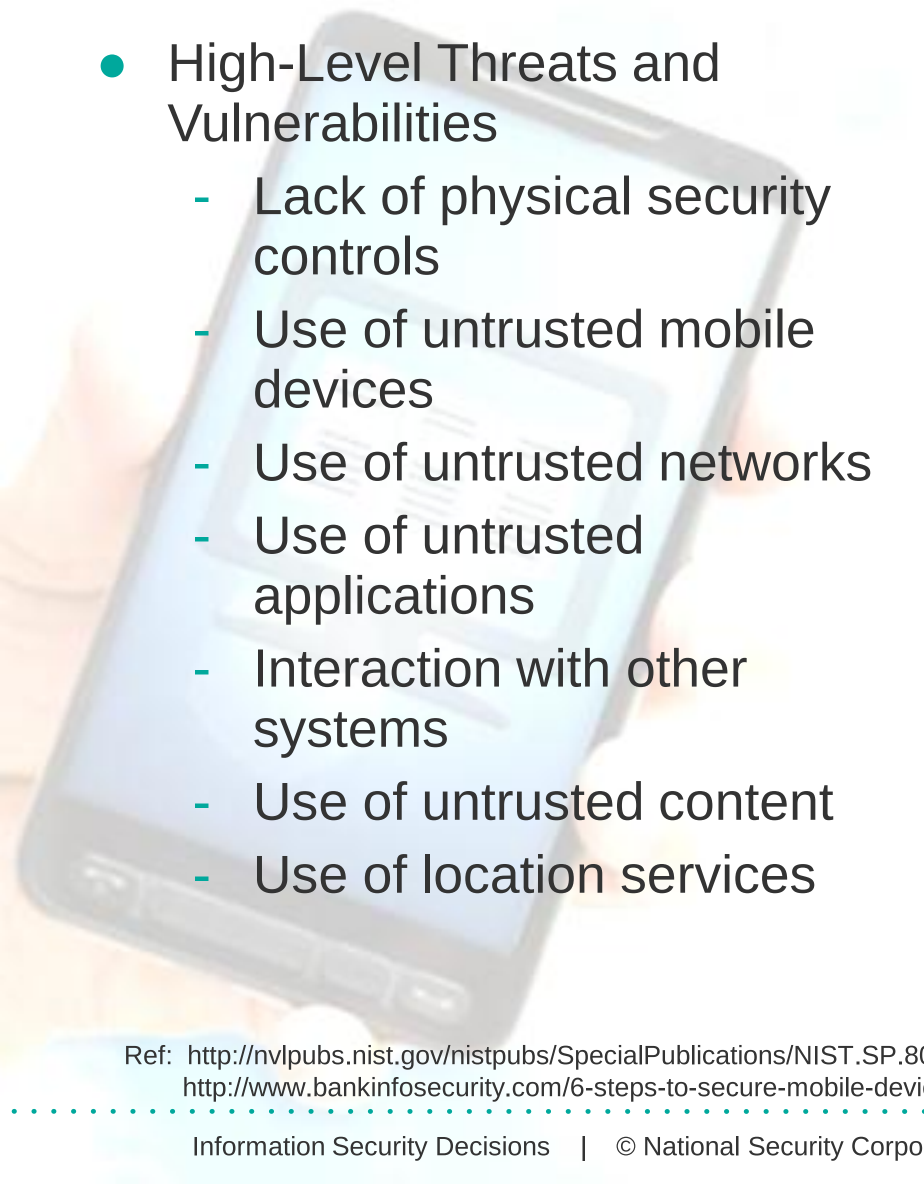


# GAO Report 12-757 - INFORMATION SECURITY: Better Implementation of Controls for Mobile Devices Should Be Encouraged

- Enable passwords in all mobile devices
- Require two-factor authentication for sensitive transactions from mobile devices
- Encrypt mobile device wireless transmissions
- Detect, remove, and block mobile malware
- Install security software in mobile devices
- Update and patch mobile device operating system
- Update and patch mobile device applications
- Limit Internet connections with mobile device firewall
- Do not “jailbreak” or “root” mobile devices
- Do not connect to unsecured WiFi network

Ref: http://www.gao.gov/products/GAO-12-757
http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html

# NIST SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise



- High-Level Threats and Vulnerabilities
  - Lack of physical security controls
  - Use of untrusted mobile devices
  - Use of untrusted networks
  - Use of untrusted applications
  - Interaction with other systems
  - Use of untrusted content
  - Use of location services

- Major Steps to Secure Enterprise Environment
  - Have mobile device security policy
  - Develop system threat models
  - Acquire solutions that provide necessary services
  - Implement and test before putting into production
  - Secure each device before permitting use
  - Regularly maintain mobile device security

Ref: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
http://www.bankinfosecurity.com/6-steps-to-secure-mobile-devices-in-enterprise-a-5857

# Top 8 Mobile Device Security Steps
# (for people who are serious about mobile security)

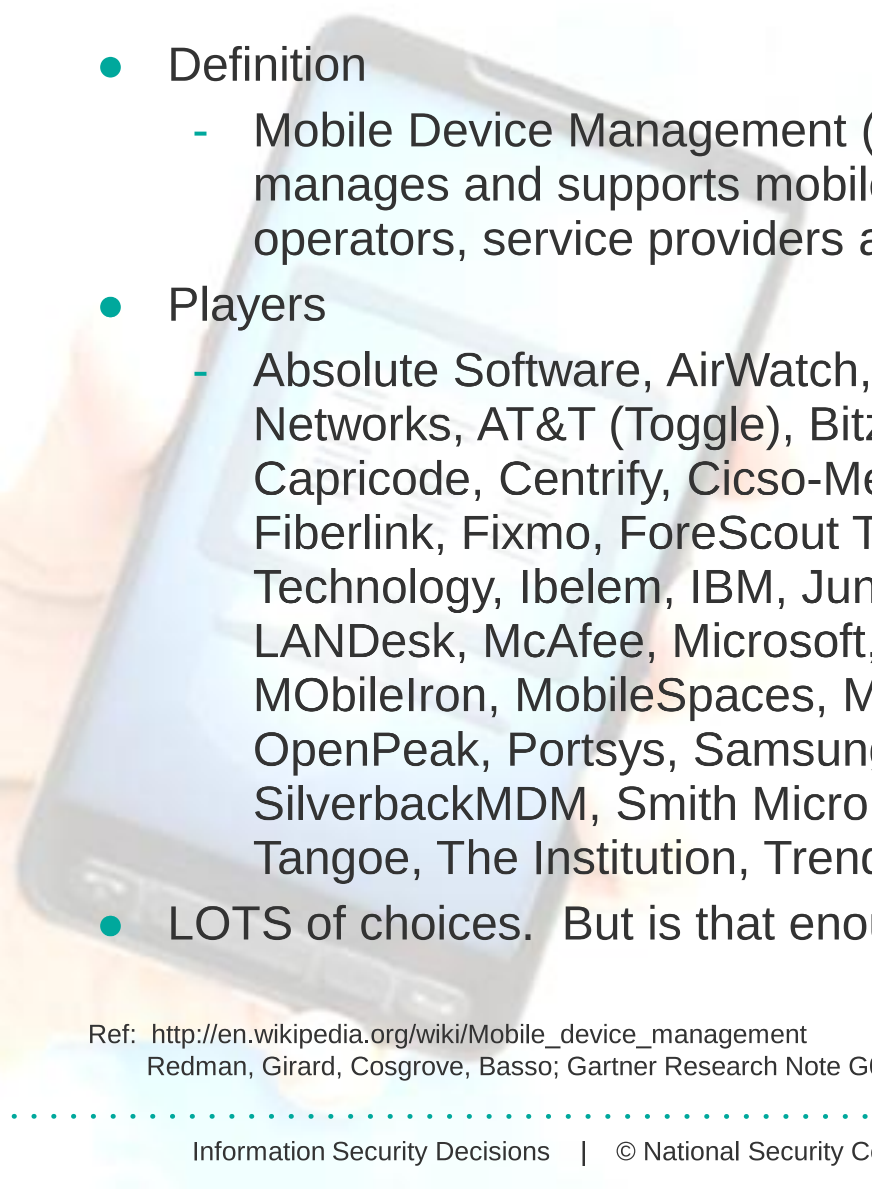
- Enforce D\device passcode authentication
- Monitoring mobile device access and use
- Patching mobile devices
- Prohibit unapproved third-party application stores
- Disable developer debug access
- Evaluate application security compliance
- Prepare an incident response plan for lost or stolen mobile devices
- Implement management and operational support

Ref: Crowley, Wright, Top 8 Steps for Effective Mobile Security, 2012

# Okay, So What Are You SUPPOSED To Do?

- Whenever possible,
  AUTOMATE GOOD BEHAVIOR
- The solution space is called
  Mobile Device Management (MDM)
- Vendors have been developing product suites for some time
  - Over 100 vendors

# What is Mobile Device Management (MDM)?



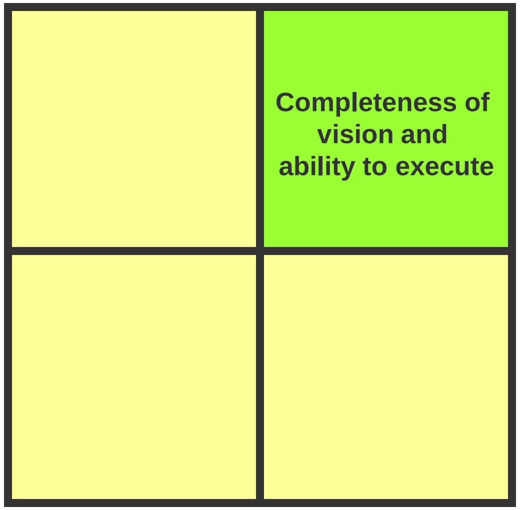
- Definition
  - Mobile Device Management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises.
- Players
  - Absolute Software, AirWatch, Amtel, Apperian, AppSense, Aruba Networks, AT&T (Toggle), Bitzer Mobile, BlackBerry, BoxTone, Capricode, Centrify, Cicso-Meraki, Citrix, Cortado, Dell Kace, Excitor, Fiberlink, Fixmo, ForeScout Technologies, Globo Mobile, Good Technology, Ibelem, IBM, Juniper Networks, Kaspersky Lab, Kony, LANDesk, McAfee, Microsoft, Mobile Active Defense, MobileFrame, MObileIron, MobileSpaces, Mobiquant, Notify Technology, Novell, OpenPeak, Portsys, Samsung SDS, SAP, Seven Principles, SilverbackMDM, Smith Micro Software, Sophos, Soti, Symantec, Tangoe, The Institution, Trend Micro, VMware
- LOTS of choices. But is that enough?

Ref: http://en.wikipedia.org/wiki/Mobile_device_management
Redman, Girard, Cosgrove, Basso; Gartner Research Note G00249820, 2013

# Chasing the “Magic”

Gartner “Magic Quadrant” vendors over last four years:

- 2010: McAfee, Sophos, CheckPoint, Symantec
- 2011: Good Technology, Sybase, AirWatch, MobileIron
- 2012: MobileIron, AirWatch, Fiberlink, Zenprise, Good Technology
- 2013: AirWatch, MobileIron, Citrix, SAP, Good Technology, Fiberlink



Completeness of vision and ability to execute

ref: “Magic Quadrant for Mobile Device Management Software
(Girard, Ouellet, Gartner Research Note G00205929, 2010)
(Redman, Girard, Wallin; Gartner Research Note G00211101, 2011)
(Redman, Girard, Basso; Gartner Research Note G00230508, 2012)
(Redman, Girard, Cosgrove, Basso; Gartner Research Note G00249820, 2013)

# We're Starting to See Some Convergence in MDM Capability "Extensions"

- For example: BlackBerry® Enterprise Service 10
  - Features include:
    - Mobile Device Management (MDM)
    - Security
    - Unified communications
    - Application management products and services
  - Manages corporate and personal-owned devices running:
    - BlackBerry OS
    - BlackBerry® 10
    - iOS
    - Android™
- But is that enough to make you want to buy BlackBerry?

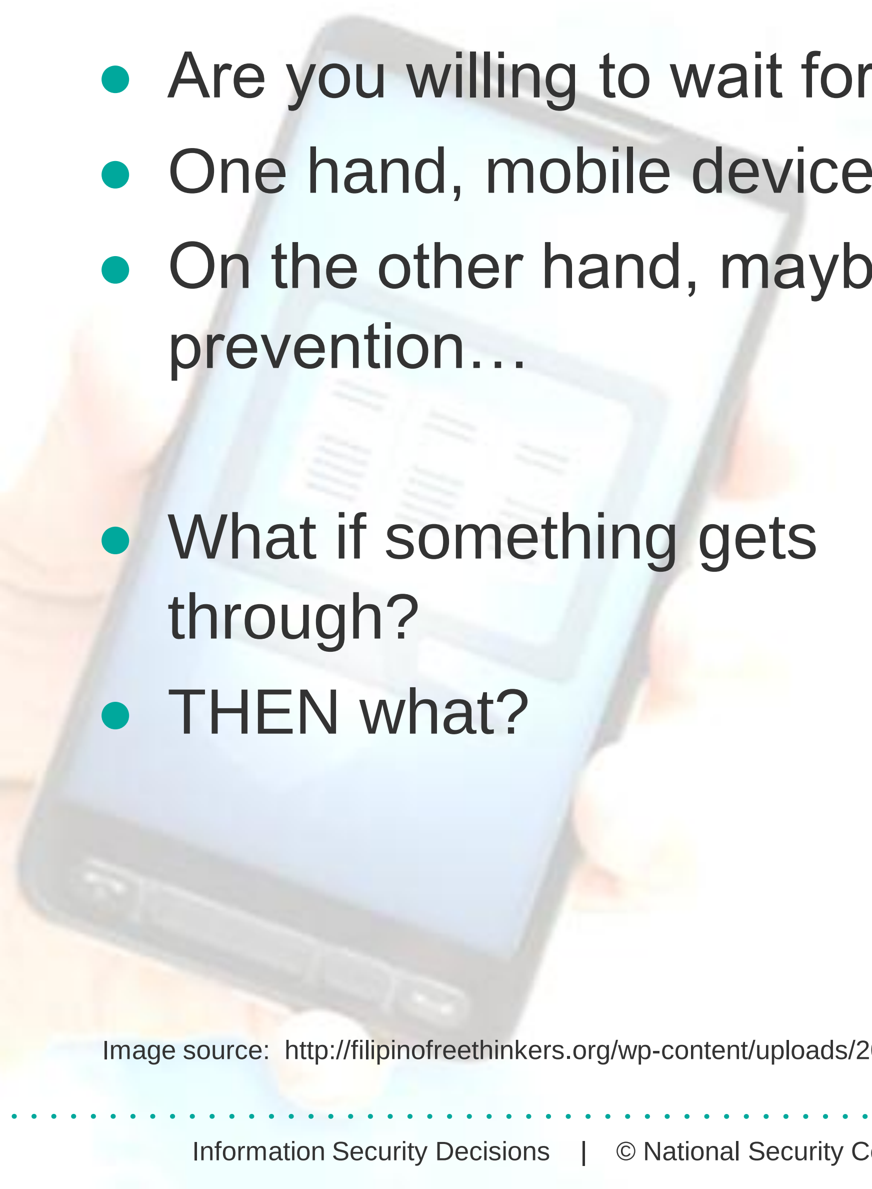
Ref: http://us.blackberry.com/content/dam/blackBerry/pdf/BB10-BES10-Enterprise-FAQ.pdf

# Where Are We Going with Endpoint Protection Platforms (EPP)?

- "Integrated protection and management ... of mobile devices ... are still rare, but will be critical future capabilities..."
- "As mobile devices become more capable, we see protection for these devices as becoming a key future requirement of EPP."
- "Longer term, we anticipate that MDM-like functionality will blend fully with EPP functionality..."

Ref: "Magic Quadrant for Endpoint Protection Platforms" - (Firstbrook, MacDonald, Girard, Gartner Research Note G00219355, 16 Jan 2012)
"Magic Quadrant for Endpoint Protection Platforms" - (Firstbrook, Girard, MacDonald, Gartner Research Note G00239869, 2 Jan 2013)

# But is Endpoint Protection the Right Marriage?



- Are you willing to wait for “longer term”?
- One hand, mobile devices ARE the endpoint
- On the other hand, maybe it’s more than just prevention…
- What if something gets through?
- THEN what?

Image source: http://filipinofreethinkers.org/wp-content/uploads/2011/03/Shotgun-marriages.jpg Fair use claimed under 17 U.S.C. 107

# Two Families of MDM are Available

- Software-based MDM
  - AirWatch
  - Good
  - MobileIron
- Automated device provisioning; works well in centralized environment
- Best suited for corporate-provided devices

- Network-based MDM
  - AeroHive
  - Aruba
  - Cisco
- Can "snapshot" device to identify presence of malware, rooting/jailbreaking
- Well-suited for BYOD

This is not an either-or choice
It's a combination of complementary technologies

Ref: https://www.nemertes.com/blog/network-based-mobile-device-management-transformation-nac

# “Prevention is Ideal, but Detection is a Must”

-Dr. Eric Cole

-Founder, Secure Anchor Consulting

# Key Questions to Support Governance, Risk, and Compliance (GRC)

- What operational risks affect business processes and requirements?
- What is the consequence of a threat or vulnerability to the set of infrastructure and applications delivering a business service?
- What compliance mandates apply?
- What combination of policies, processes and controls are best suited to measure, mitigate or reduce risks and vulnerabilities, and contribute to compliance?
- What tools will effectuate and automate security controls?
- Is the risk reduction cost-effective? Does it optimize resources?

Ref: Hardy, G. Mark, “The Critical Security Controls:
What’s NAC Got to Do With It?, 2013, 4

# Hierarchy of Needs

## We must manage RISK

- Risk = Threat x Vulnerability x Asset Value

## Goal:  manage risk by reducing exposure

## We do so with CONTROLS

- Technical controls – affects computer systems
  - Implement with software or hardware
- Administrative controls – affects people and organization
  - Implement with policy and procedures
- Physical controls – affects environment and devices
  - Implement with equipment and add-ons

## Let’s look further at technical controls…

# Lots of Choices … Maybe?

- Problem:  most enterprises are aware of only 80 percent of the devices on their networks
  - Many endpoints are unmanaged, unprotected or unknown
- There are multiple strategies for implementing technical controls
  - Mobile Device Management (MDM)
  - Network Access Control (NAC)
  - Virtual application containers
  - Virtual Device Interface (VDI)
- Recent survey shows most organizations forgo technical solutions and rely on user education for prevention

Ref:  “Strategic Roadmap for Network Access Control,” Gartner, October 2011, by Lawrence Orans and John Pescatore.
www.sans.org/reading_room/analysts_program/SANS-survey-mobility.pdf

# “Classic” Network Access Control

## Communications between server and managed endpoint

## Early NAC:  802.1X (IEEE:2001)

- Supplicant provides credentials
- Authenticator forwarc
- Server verifies creder
- If valid,
  access granted
- If not,
  access denied

## But …
## is that ENOUGH?

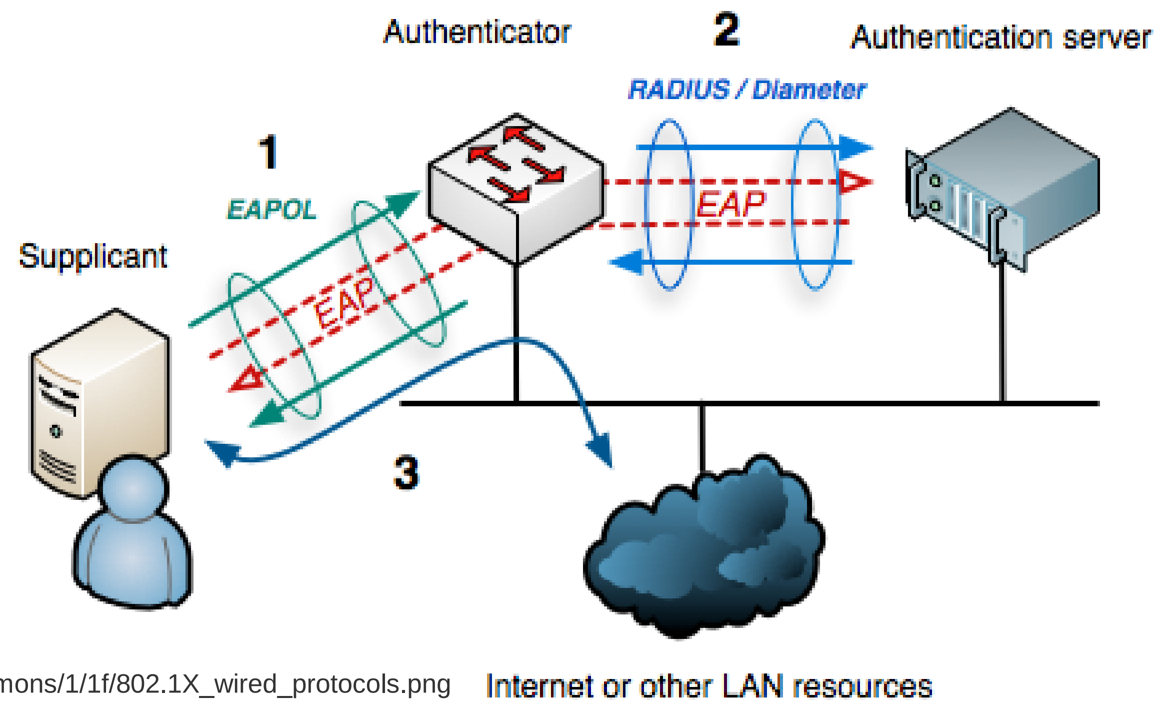


Image source:  http://upload.wikimedia.org/wikipedia/commons/1/1f/802.1X_wired_protocols.png

# What Could Possibly Go Wrong?  Go Wrong?  Go Wrong?

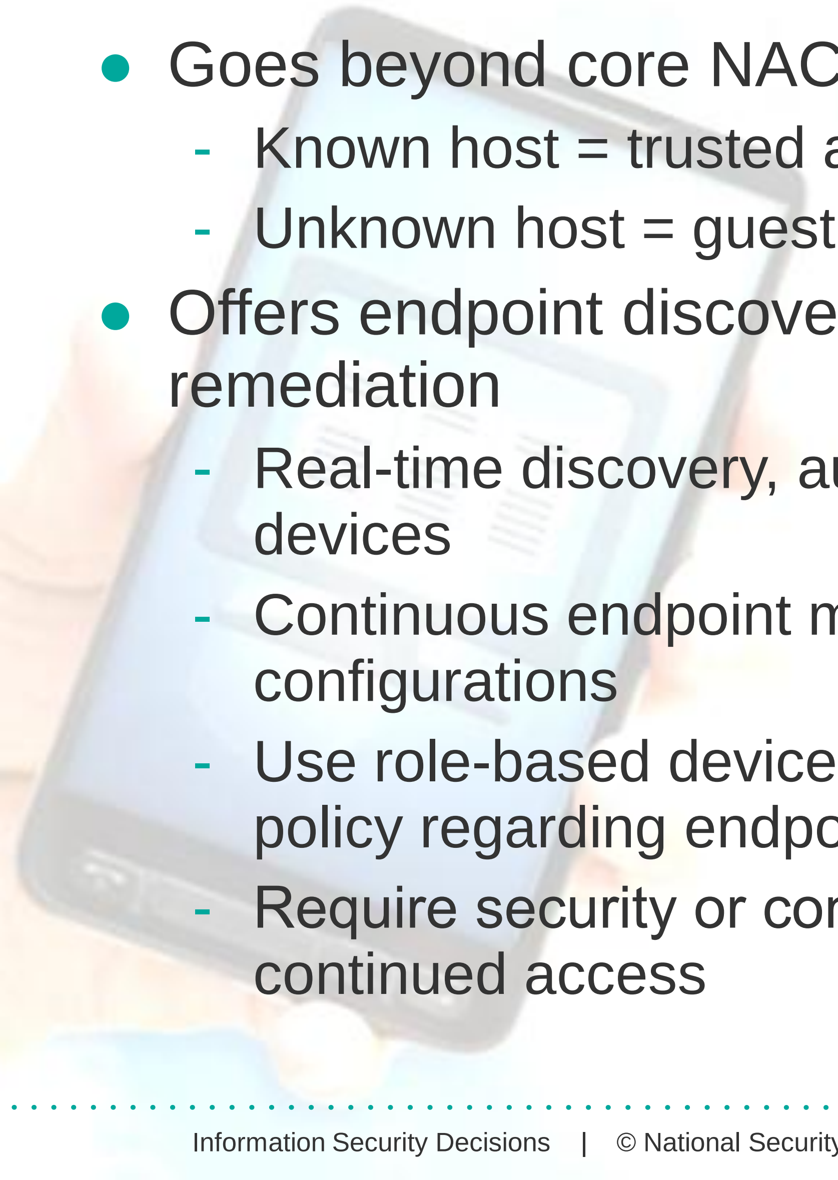
- What about non-standard device configurations?
- What about insecure configurations?
- What about zero-day attacks?
- What about unauthorized applications?
- What about network-enabled printers?
  - That later try to attack your servers?
- What about other unmanaged devices?
- What about devices with no management client?
- And … what about Naomi?

Obscure reference to Love of Chair, 1972 season of The Electric Company, copyright The Children's Television Network, fair use clamed under 17 USC 107

# Access Decisions are More than Just YES/NO

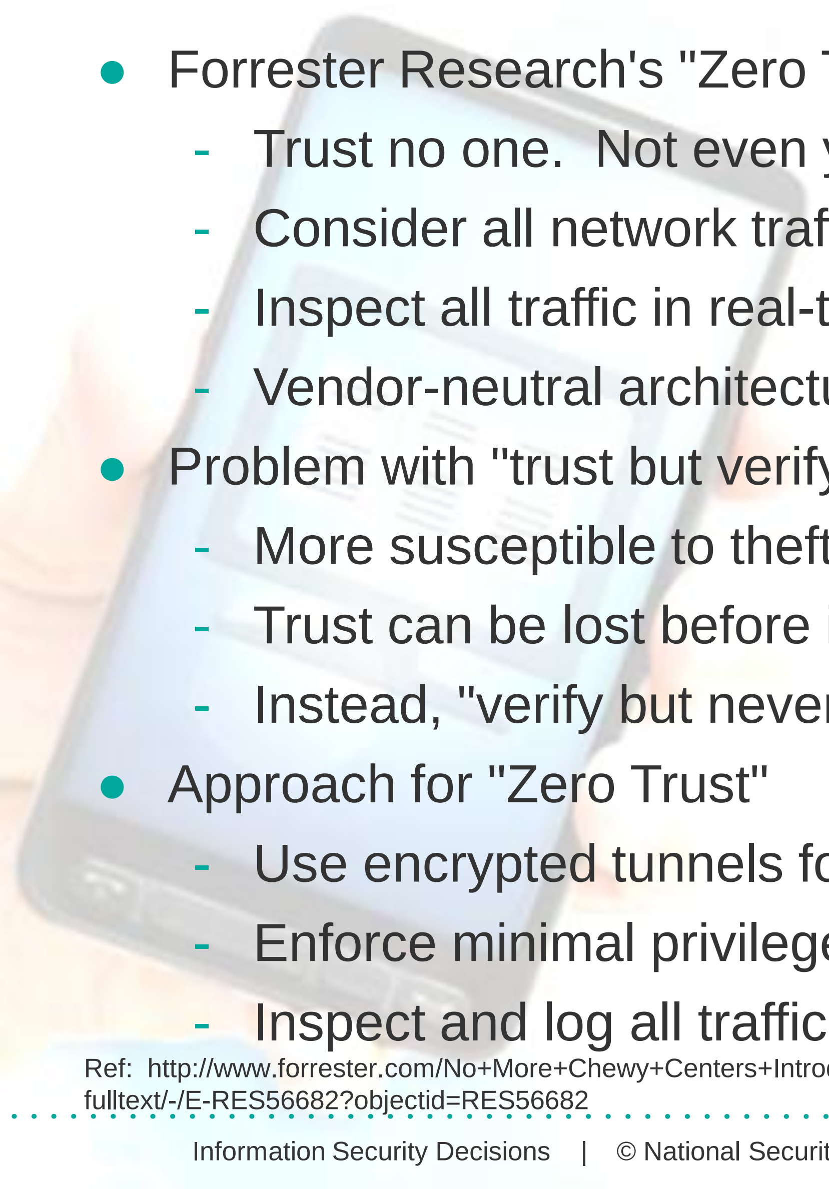
- Attaching devices may or may not have an 802.1X client
  - Works well for previously registered and configured devices
  - Not so well for *ad hoc* connections or new equipment
- Just because a device connects doesn’t mean it should access all resources
  - Visitors can/should be shunned to a guest network
  - Certain devices should be restricted to certain access
    - Medical information only available to specific devices
  - Make determination based on combination of user ID and device ID
    - What about a trusted user coming from an untrusted device?
  - What if a trusted device shows up with malware?

# What is Next-Generation NAC?



- Goes beyond core NAC function
  - Known host = trusted access
  - Unknown host = guest access
- Offers endpoint discovery, assessment, enforcement and remediation
  - Real-time discovery, authentication and classification of devices
  - Continuous endpoint monitoring and mitigation of incorrect configurations
  - Use role-based device inspection and enforce granular policy regarding endpoint configuration
  - Require security or configuration “fixes” as condition for continued access

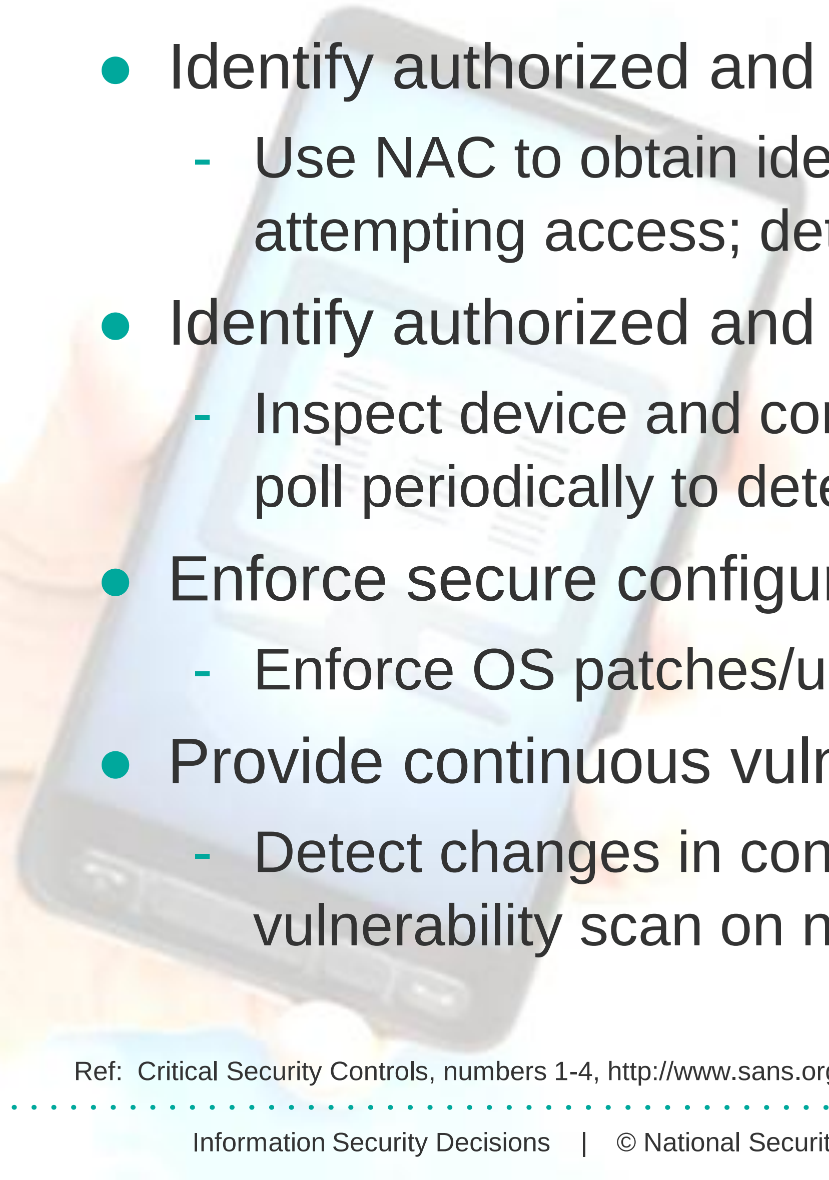
# Not Everyone Agrees with NAC As Primary Strategy



- Forrester Research's "Zero Trust" Model (John Kindervag):
  - Trust no one.  Not even your insiders.
  - Consider all network traffic untrusted
  - Inspect all traffic in real-time
  - Vendor-neutral architecture
- Problem with "trust but verify" with mobile devices:
  - More susceptible to theft and human error
  - Trust can be lost before it is reported
  - Instead, "verify but never trust"
- Approach for "Zero Trust"
  - Use encrypted tunnels for internal and external networks
  - Enforce minimal privilege and strict access control
  - Inspect and log all traffic

Ref:  http://www.forrester.com/No+More+Chewy+Centers+Introducing+The+Zero+Trust+Model+Of+Information+Security/fulltext/-/E-RES56682?objectid=RES56682

# NAC in the BYOD Environment



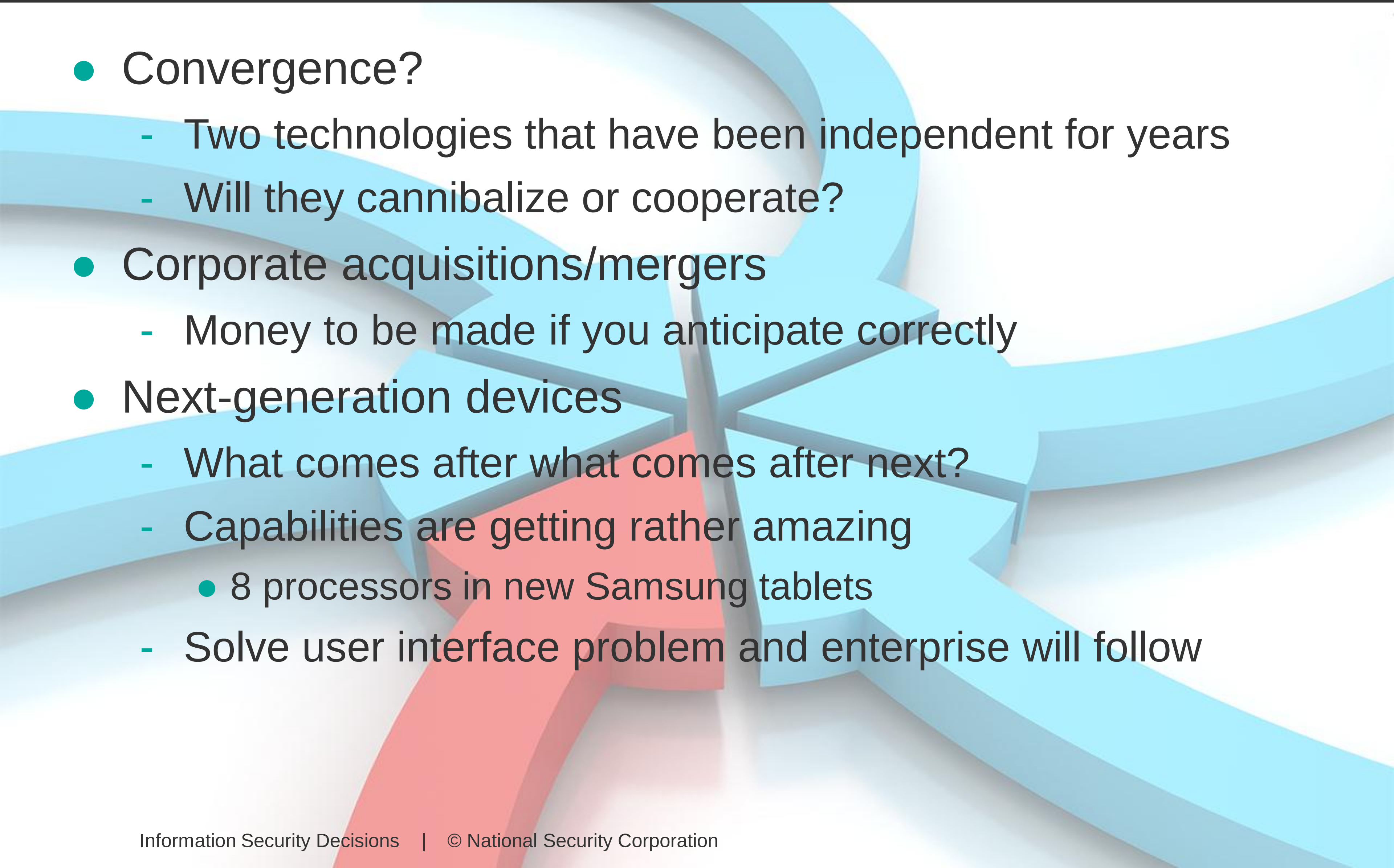
- Identify authorized and unauthorized devices
  - Use NAC to obtain identity of user and BYOD device attempting access; determine permitted access; log or alert
- Identify authorized and unauthorized software
  - Inspect device and compare configuration against policy; poll periodically to detect changes; interdict if needed
- Enforce secure configuration of BYOD device
  - Enforce OS patches/updates before permitting full access
- Provide continuous vulnerability assessment
  - Detect changes in configuration or behavior, initiate vulnerability scan on newly connecting BYOD devices

Ref: Critical Security Controls, numbers 1-4, http://www.sans.org/critical-security-controls

# Putting MDM and NAC together

- MDM
  - Policy and configuration management for mobile handhelds
  - Solution for securing mobile users and content
- NAC
  - Inspect and remediate devices when connecting to network
  - Facilitate, monitor, and interdict access as appropriate
- Coordinate
  - Lower enterprise risk with more comprehensive solution
- Vendor cooperation?
  - Maybe

# Future and Conclusions



- Convergence?
  - Two technologies that have been independent for years
  - Will they cannibalize or cooperate?
- Corporate acquisitions/mergers
  - Money to be made if you anticipate correctly
- Next-generation devices
  - What comes after what comes after next?
  - Capabilities are getting rather amazing
    - 8 processors in new Samsung tablets
  - Solve user interface problem and enterprise will follow

# Thank you!

## Questions?

G. Mark Hardy, CISSP, CISM
President, National Security Corporation
gmhardy@nationalsecurity.com
+1.410.933.9333

TechTarget | TechTarget Speaker Bureau 2013