Healthcare Mobility

Moving Forward in an Ever-Changing Industry

Ernest Dunn
Director, Secure Networks
CISSP-ISSMP, CISA, CISM, CRISC, CCNP-Security
CISCP, CNDA, CEH, ECSA, RSA CSE, SFCP,TPCSE, FCA

Lisa Owens, MBA, PMP
Director, Healthcare Industry Solutions

PRESIDIO™

QUICK FACTS

- Local presence in **50 offices** & Global scale – **5,000+** clients in U.S., Europe & Asia
- **2500 employees** – 1000 are highly certified consulting engineers with **3500** certifications
- Multi billion dollar privately held company with **exceptionally strong balance sheet**
- Market leadership validated by double-digit annual growth rates for **15+ years**
- **1,350 Healthcare organizations** serviced
- Passion for driving client results – **95% client retention**, best-in-class client satisfaction
- Deep, strategic **partnerships** with leading innovators in the IT industry

Session Objectives

- Understand how a clinical mobility strategy can help drive clinical integration
- Define the key considerations for implementing a comprehensive clinical mobility strategy
- Review emerging healthcare security threats and risks related to Mobile Health solutions
- Discuss Presidio's Mobile Security Architecture

Only the Tip of the Iceberg

- Enterprise Mobility Market expected to reach $340 BILLION by 2017
- 80% of Physicians use smartphones and medical apps
- Estimated more than 17 million wearable bands will ship this year
- 320 million mobile phones and 1.7 million hospital beds in the U.S. = 185 phones per bed

The Nexus of Disruptive Forces

- Consumerization of Technology
- EMR Adoption
- Ubiquitous Computing
- Security Compliance

More than a Mobility Trend

- New models of care are being adopted as healthcare costs continue to increase
- Specialist and clinician shortages requiring productivity improvements
- Need for better access to care for patients and providers
- Growing interest in providing patients with engagement and collaboration options
- Increasing demand for personalized care, wellness programs and education

Driving Clinical Integration with Mobility

Clinical Mobility Infrastructure Checklist

- Connectivity √
- Performance √
- Manageability √
- Usability √
- Scalability √
- Security √

Healthcare Mobile Use Cases

PRESIDIO™

MOBILE HEALTH THREATS

Top of Mind IT Security Concerns

- How do I understand the security posture of popular personal devices and user apps?
- How do I ensure compliance with PCI, HIPAA, FISMA, etc?
- How do we segment BYOD, partners, consultants and guests?
- How do I enable patient control over the data they provide while using a mobile app?

PRESIDIO™

Healthcare - Patient Data Lost

- **90% of Hospitals and Clinics exposed or lost patients data in 2012 and 2013** according to Ponemon Institute study
- **No industry hit harder** by data breaches
- Attractive to hackers
  - Medical records $50 each
  - Credit cards $1 each
- Tons of outdated equipment
- Many organizations not encrypting data

Medical faces more data breaches than military and banking sectors combined

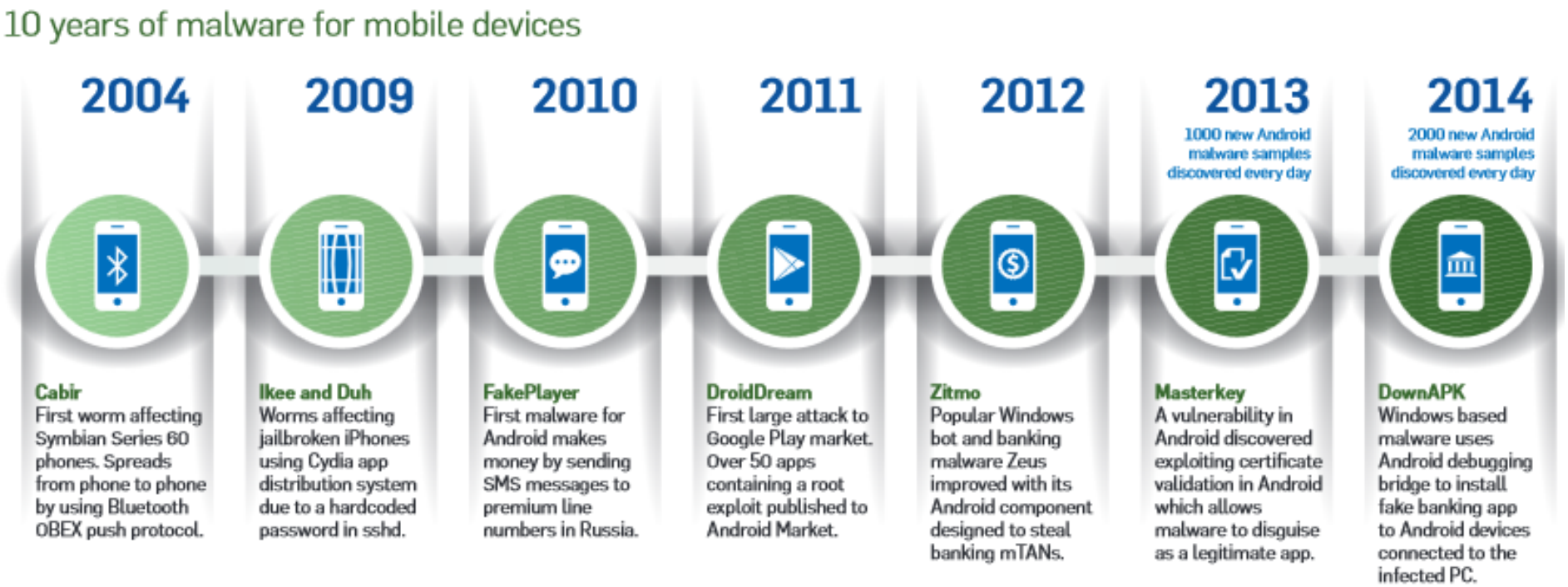
PRESIDIO™

The average cost of a security breach to a company was **$3.5 million** and 15 percent more than what it cost last year.

- 2014 Cost of Data Breach Study: Global Analysis

PRESIDIO™

Mobile Malware

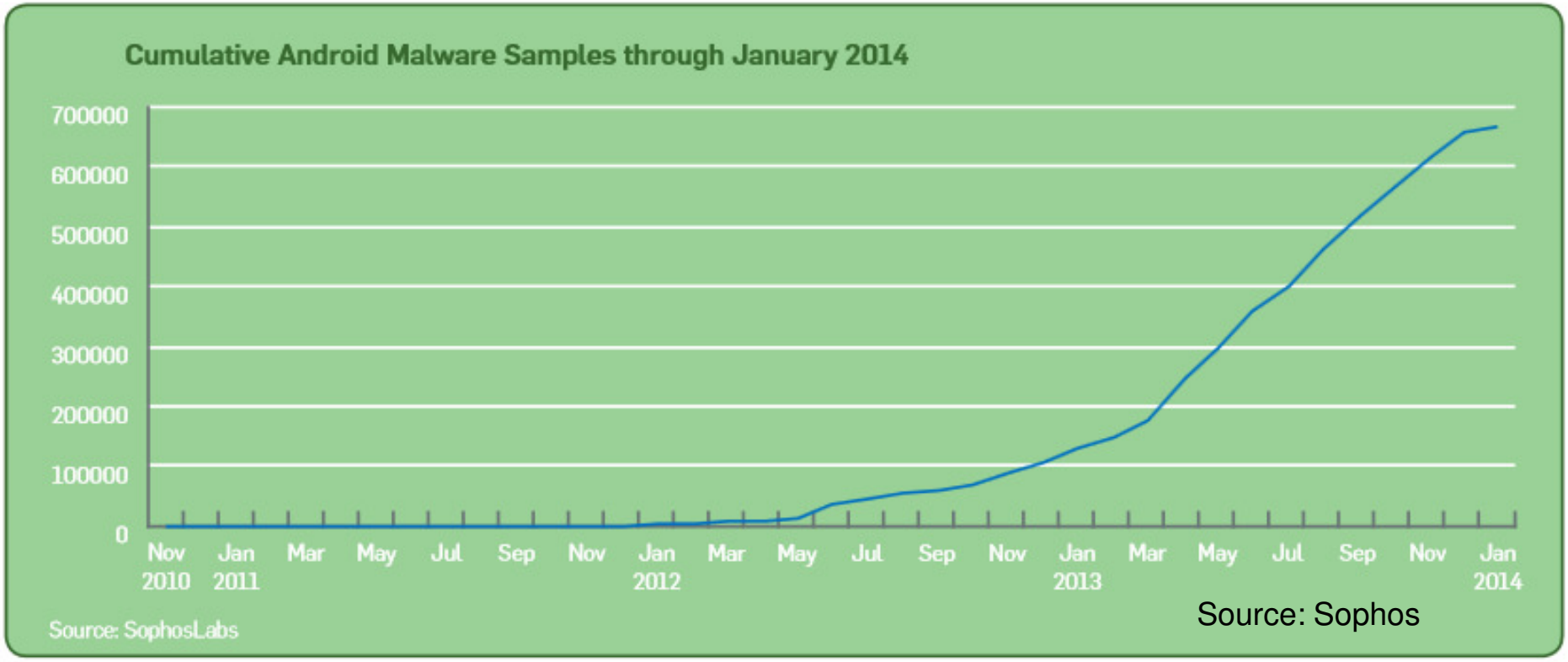


Source: Sophos

PRESIDIO™

Android Malware

- 97% of mobile malware discovered in 2014 was targeted at Android
- 1 out of every 10 Android apps contain malware
- Android malware up 600% this year



Source: Sophos

PRESIDIO™

Mobile Market share

- **866 million Android devices will ship this year** (up from 505 million last year.
- **296 million iOS** devices will ship (up from 212 million last year)
- **339 million Windows devices will ship** (a slight dip from 346 million last year)**.**
- **Next year Android is likely to see a billion devices shipped, with** 378 million Windows devices and 354 million iOS devices. **- Gartner**

PRESIDIO™

Top 5 Mobile Threats

1. Lost or stolen device
2. Mobile malware – data leakage
3. Wi-Fi hotspots
4. Vulnerabilities – OS and app
5. Proximity-based hacking

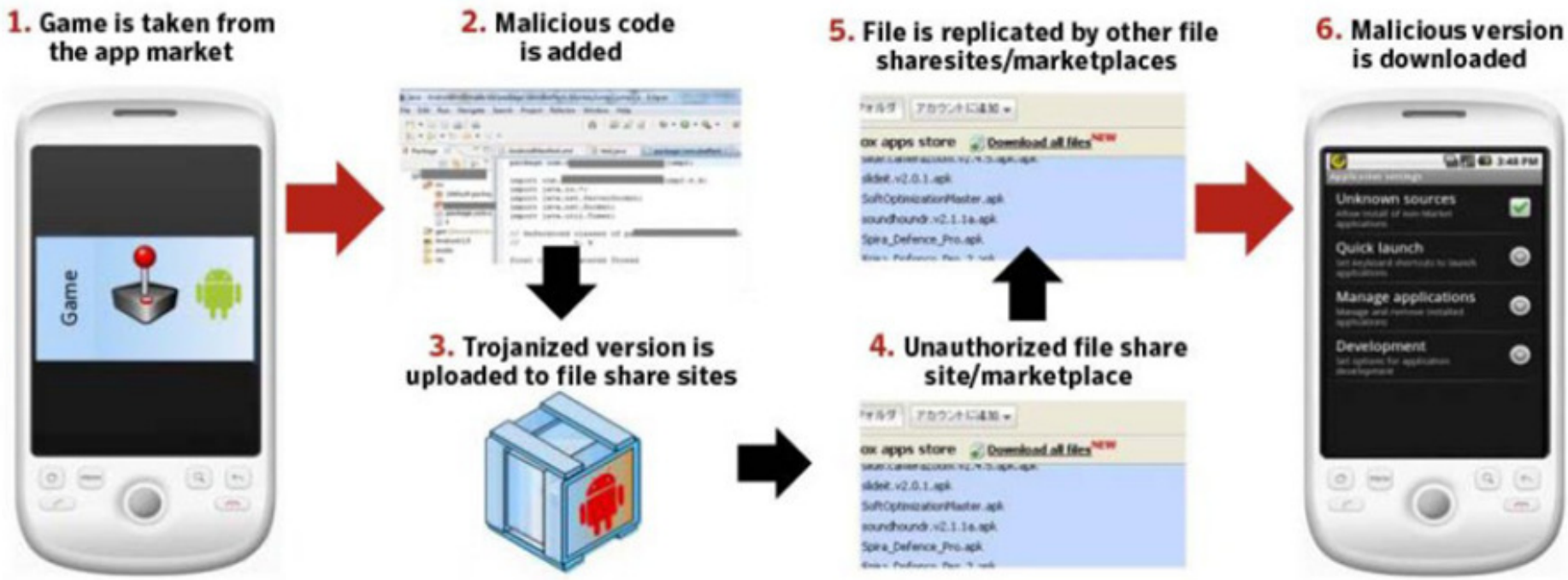
Cell phone insurance provider Asurion reports that 60 million smartphones are lost, stolen or damaged each year. In dollar terms, according to a report conducted by mobile security firm Lookout, Americans lost $30 billion dollars worth of smartphones in 2011.

Symantec conducted an experiment earlier this year where they "lost" 50 phones on purpose (msnbc.com):

- 43 percent of finders clicked on an app labeled "online banking."
- 53 percent clicked on a filed named "HR salaries."
- 57 percent opened a file named "saved passwords“.
- 60 percent checked Social networking tools and personal e-mail.
- 72 percent tempted a folder labeled "private photos“.
- 89 percent clicked on something they probably shouldn’t have.
- 50 percent of the phones were returned.

PRESIDIO™

How do these devices get compromised?



Main Attack Vectors

Apps - Browser, Plugins(PDF, QuickTime), Flash, Javascript, ect

Spam - 83% of spam uses URLs, malware is hosted on remote site

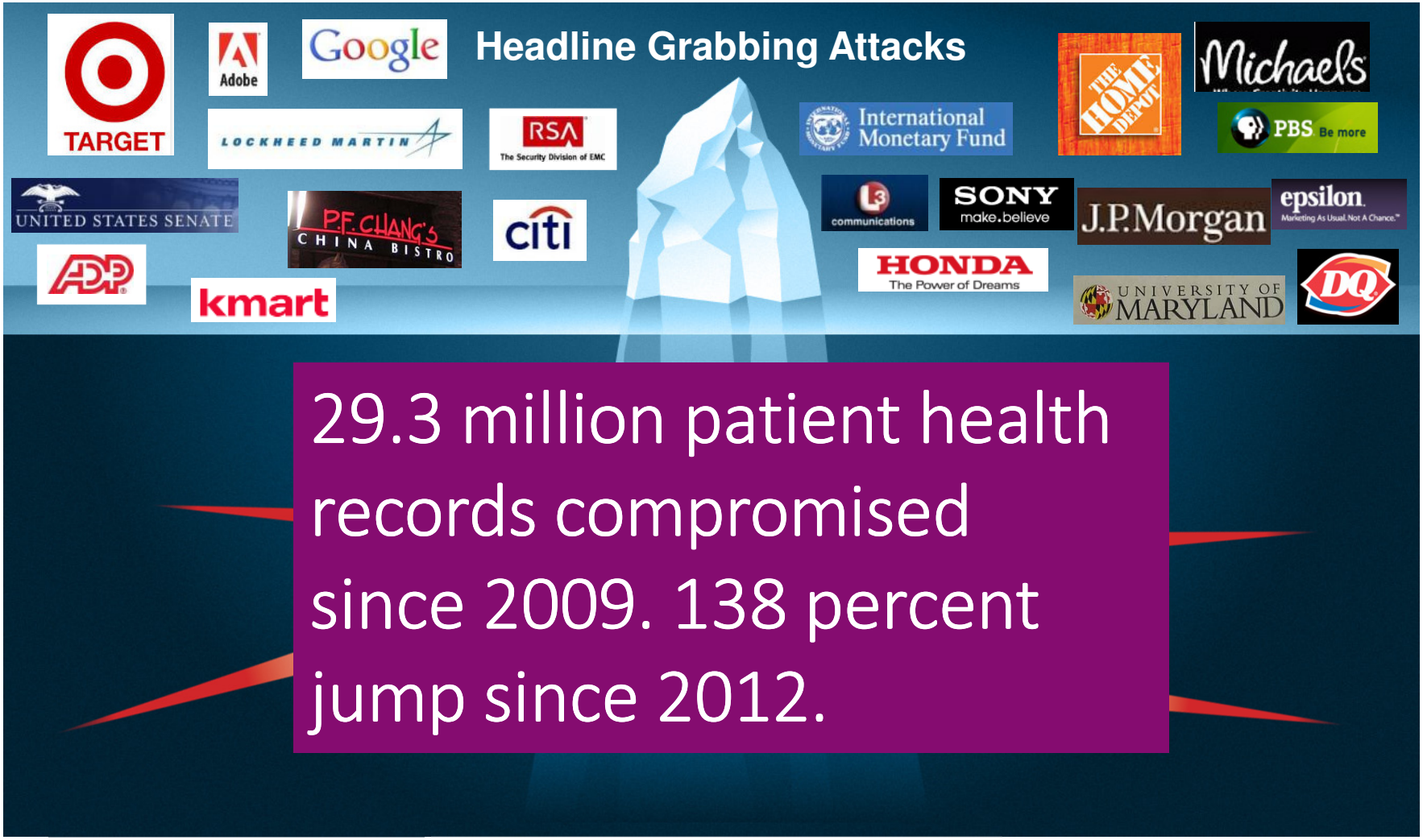
Targeted - Social Engineering and Spear Phishing

PRESIDIO™

Anatomy of a Hacked Mobile Device

PRESIDIO™

The hits keep coming…



PRESIDIO™

MOBILE SECURITY CHALLENGES

New Expectations

Changing Workspace

DEVICE PROLIFERATION

15 Billion Devices by 2015 that Will Be Connecting to Your Network

On Average Every Person Has 3–4 Devices On Them that Connect to the Network

75% of Staff Are Bringing Their Own Devices to Work

DEVICE PROLIFERATION

NEXT GENERATION WORKFORCE

VIRTUALIZATION

New Expectations

Changing Workspace

NEXT GENERATION WORKFORCE

Work Is No Longer a Place You Go to Work

People Are Willing to Take a Pay Cut as Long as They Are Able to Work from Home

70% percent of end users admit to breaking IT policy to make their lives easier

Need Anywhere, Anytime, Any Device Access

New Expectations

Changing Workspace

VIRTUALIZATION

"60% of server workloads will be virtualized by 2013"

"20% of professional PCs will be managed under a hosted virtual desktop model by 2013."

Datacenters are evolving, Applications are now objects moving through the network

DEVICE PROLIFERATION

NEXT GENERATION WORKFORCE

VIRTUALIZATION

IMPROVING MOBILE SECURITY

SANS Top 20 Controls

#	Guidelines
1	Inventory of authorized and unauthorized devices
2	Inventory of authorized and unauthorized software
3	Secure configurations for hardware and software
4	Continuous vulnerability assessment and remediation
5	Malware defenses
6	Application software security
7	Wireless device control
8	Data recovery capability (validated manually)
9	Security skills assessment and training to fill gaps
10	Secure configurations for network devices (Firewall, Router and Switch)

#	Guidelines
11	Limitation and control of network ports and services
12	Controlled use of administration privileges
13	Boundary defense
14	Maintenance, monitoring and analysis of audit logs
15	Controlled access based or need to know
16	Access monitoring and control
17	Data Loss Prevention (DLP)
18	Incident response capability
19	Secure networking engineering
20	Penetration tests and red team exercises

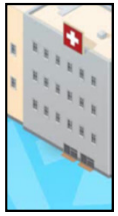
14 OUT OF 20 RELATED TO BYOD

http://www.sans.org/critical-security-controls/

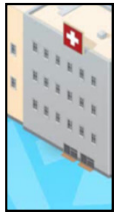
PRESIDIO™

MOBILE HEALTH SMART SOLUTION

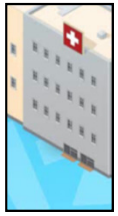
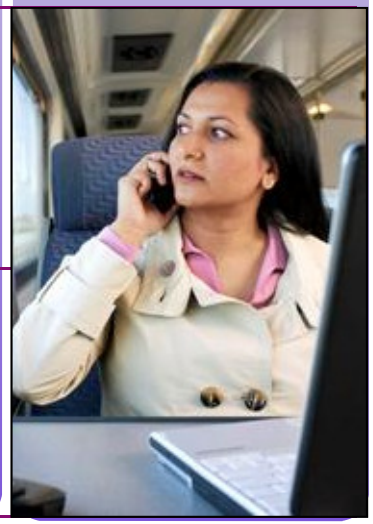
BYOD Policy Considerations

	LIMIT	BASIC	ENHANCED	ADVANCED
Business Policy	Environment Requires Tight Controls			
Device Types	Corp Only Device			
Hospital (Example) 	Hospital extends wireless access to employees for corporate devices (laptop, iPad, smartphone)			
IT Requirements	• Visibility to who/what is on network • Restrict access to only corporate issued devices			

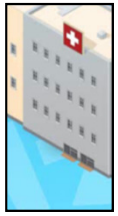
BYOD Policy Considerations

	LIMIT	BASIC	ENHANCED	ADVANCED
Business Policy	Environment Requires Tight Controls	Focus on Basic Services, Easy Access		
Device Types	Corp Only Device	Broader Device Types but Internet Only Simple Guest		
Hospital (Example) 	Hospital extends wireless access to employees for corporate devices (laptop, iPad, smartphone)	Hospital provides guest access to patients		
IT Requirements	• Visibility to who/what is on network • Restrict access to only corporate issued devices	• Restrict personal devices to public internet • Restricted access to internal sites		

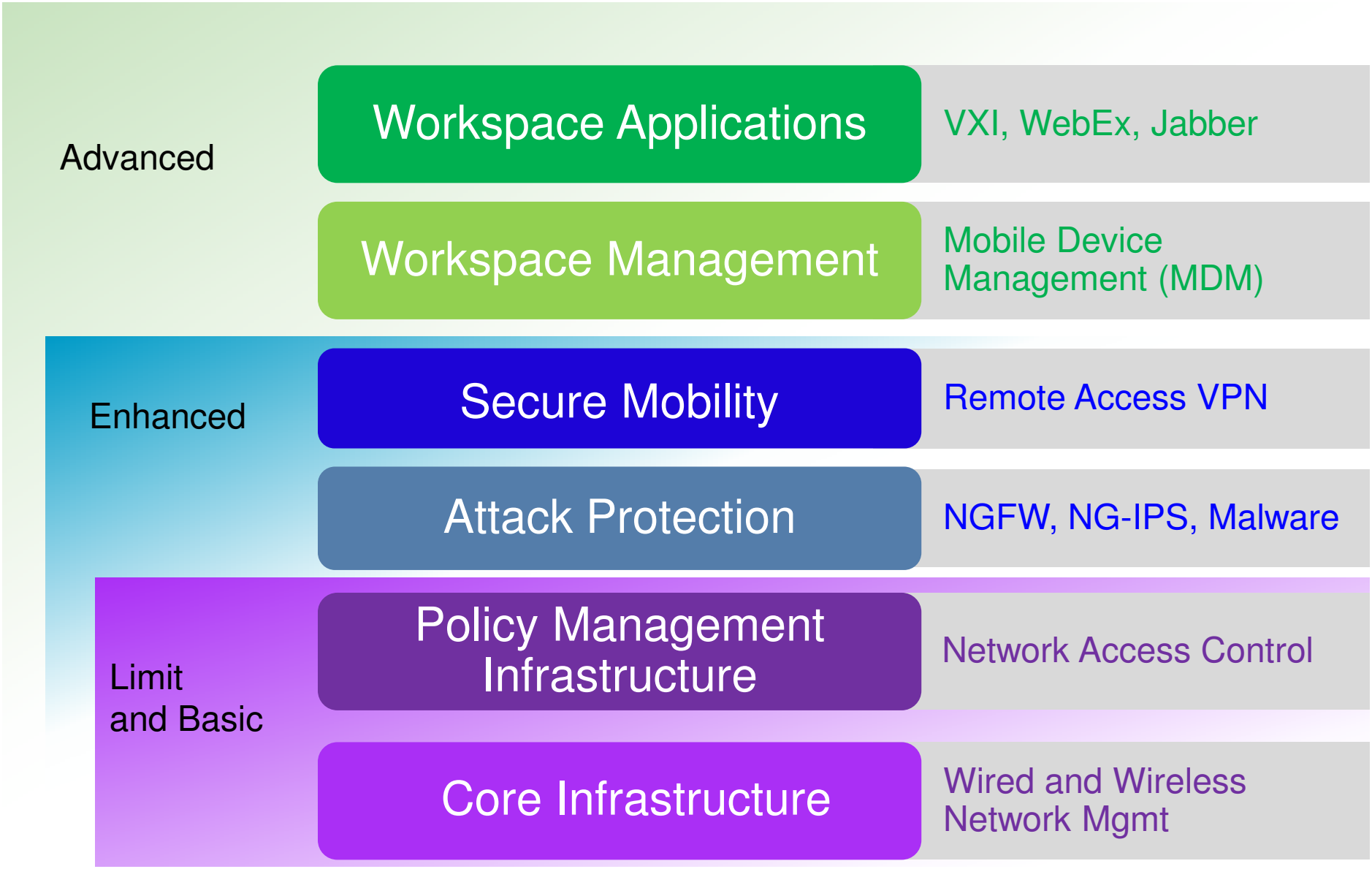
BYOD Policy Considerations

	LIMIT	BASIC	ENHANCED	ADVANCED
Business Policy	Environment Requires Tight Controls	Focus on Basic Services, Easy Access	Secure Access to Business Applications Onsite/Offsite	
Device Types	Corp Only Device	Broader Device Types but Internet Only Simple Guest	Multiple Device Types + Access Methods Early BYOD Commercial Adopters	
Hospital (Example) 	Hospital extends wireless access to employees for corporate devices (laptop, iPad, smartphone)	Hospital provides guest access to patients	Doctor uses personal device in hospital and offsite on the train with access to some hospital applications	
IT Requirements	• Visibility to who/what is on network • Restrict access to only corporate issued devices	• Restrict personal devices to public internet • Restricted access to internal sites	• Allow granular onsite and offsite access to network/applications for personal and company devices	

BYOD Policy Considerations

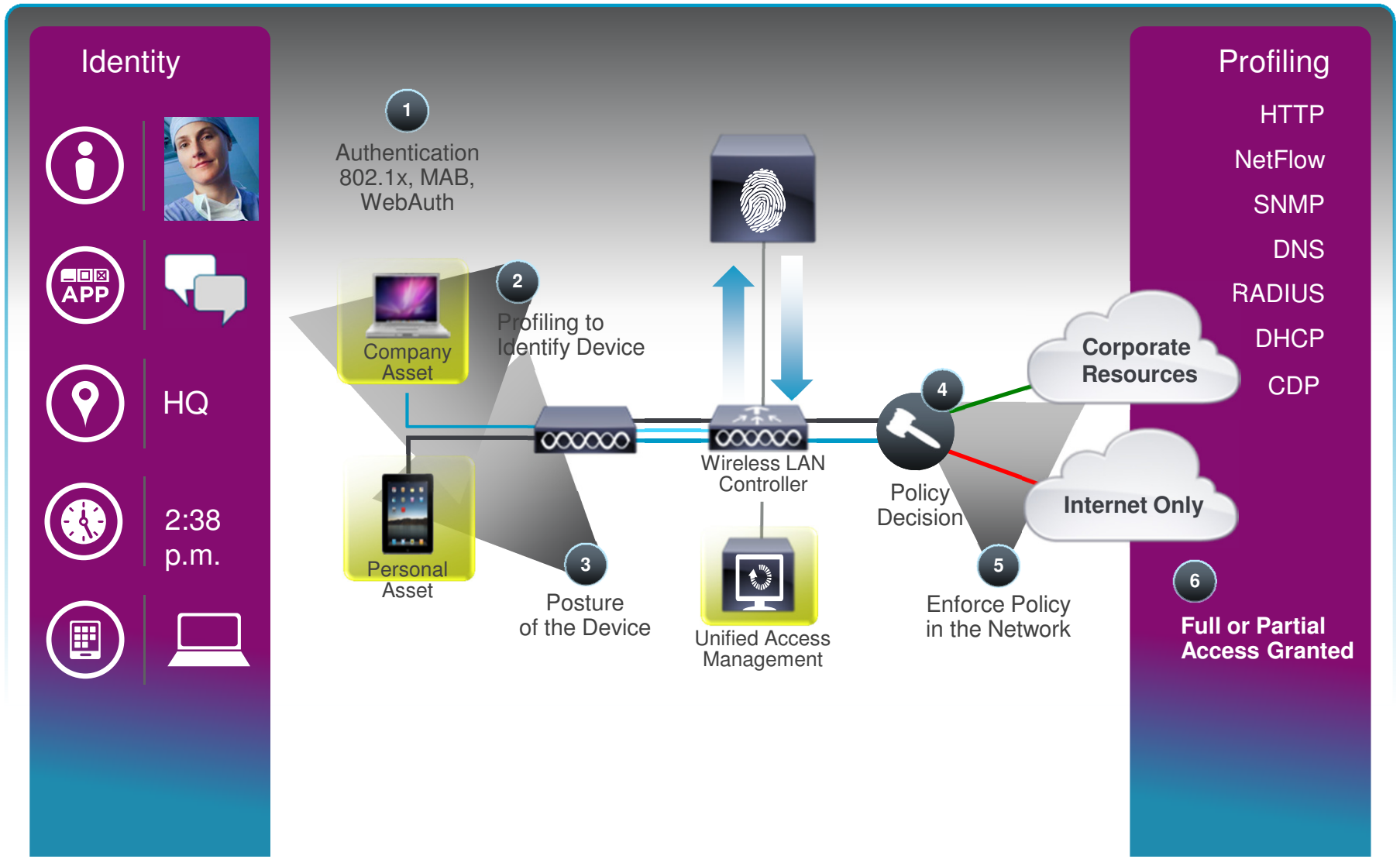
	LIMIT	BASIC	ENHANCED	ADVANCED
Business Policy	Environment Requires Tight Controls	Focus on Basic Services, Easy Access	Secure Access to Business Applications Onsite/Offsite	All Key Applications, New Services, Full Control
Device Types	Corp Only Device	Broader Device Types but Internet Only Simple Guest	Multiple Device Types + Access Methods Early BYOD Commercial Adopters	Any Device, Any Ownership Innovative Organizations
Hospital (Example) 	Hospital extends wireless access to employees for corporate devices (laptop, iPad, smartphone)	Hospital provides guest access to patients	Doctor uses personal device in hospital and offsite on the train with access to some hospital applications	Hospital administrator is granted full network access to applications with new collaboration services
IT Requirements	• Visibility to who/what is on network • Restrict access to only corporate issued devices	• Restrict personal devices to public internet • Restricted access to internal sites	• Allow granular onsite and offsite access to network/applications for personal and company devices	• Enable a full mobile and collaboration experience

Smart Solution Building Blocks



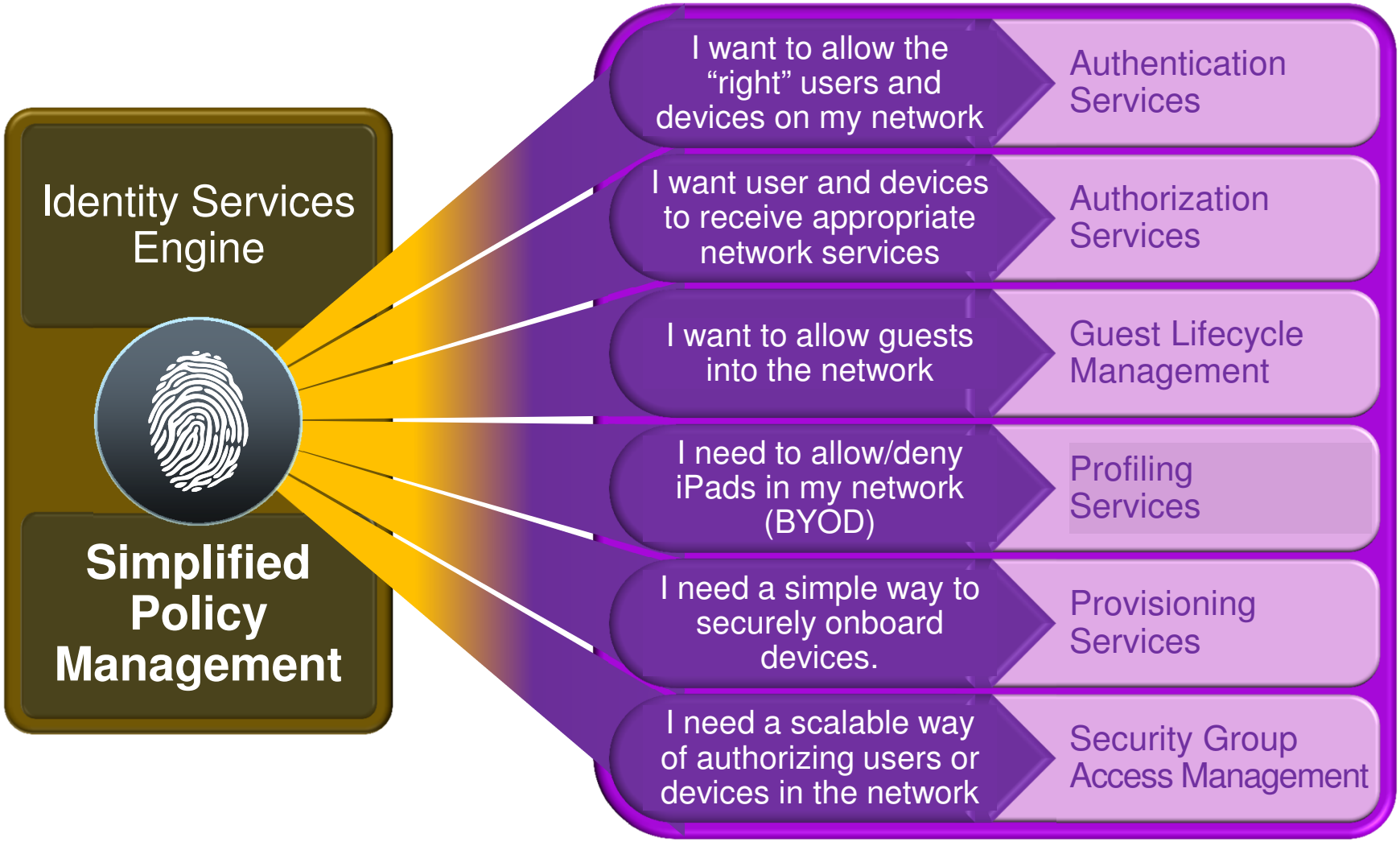
Identity and Context Awareness

Policy Management



Comprehensive NAC Solution

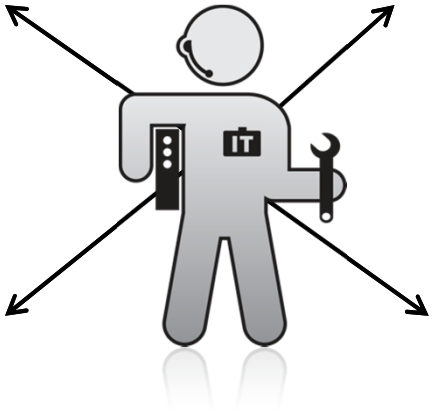
Policy Management - A System to Implement Technical Policy



Mobile Work Space - MDM

"How do I distribute apps and embrace BYOD?"

"How do I manage the explosion of OSs?"



"How do I manage security and identity across all this?"

"How do I secure and mobilize content?"

"I need to move at **consumer speed**, yet with **security** and **compliance**"

Automated Device Security

Posture Assessment and Compliance Check

Comprehensive Secure Access

- Device registration status
- Device compliance status
- **Disk encryption status**
- **Pin lock status**
- **Jailbreak status**
- **Manufacturer**
- Model
- **IMEI**
- Serial number
- **OS version**
- Phone number

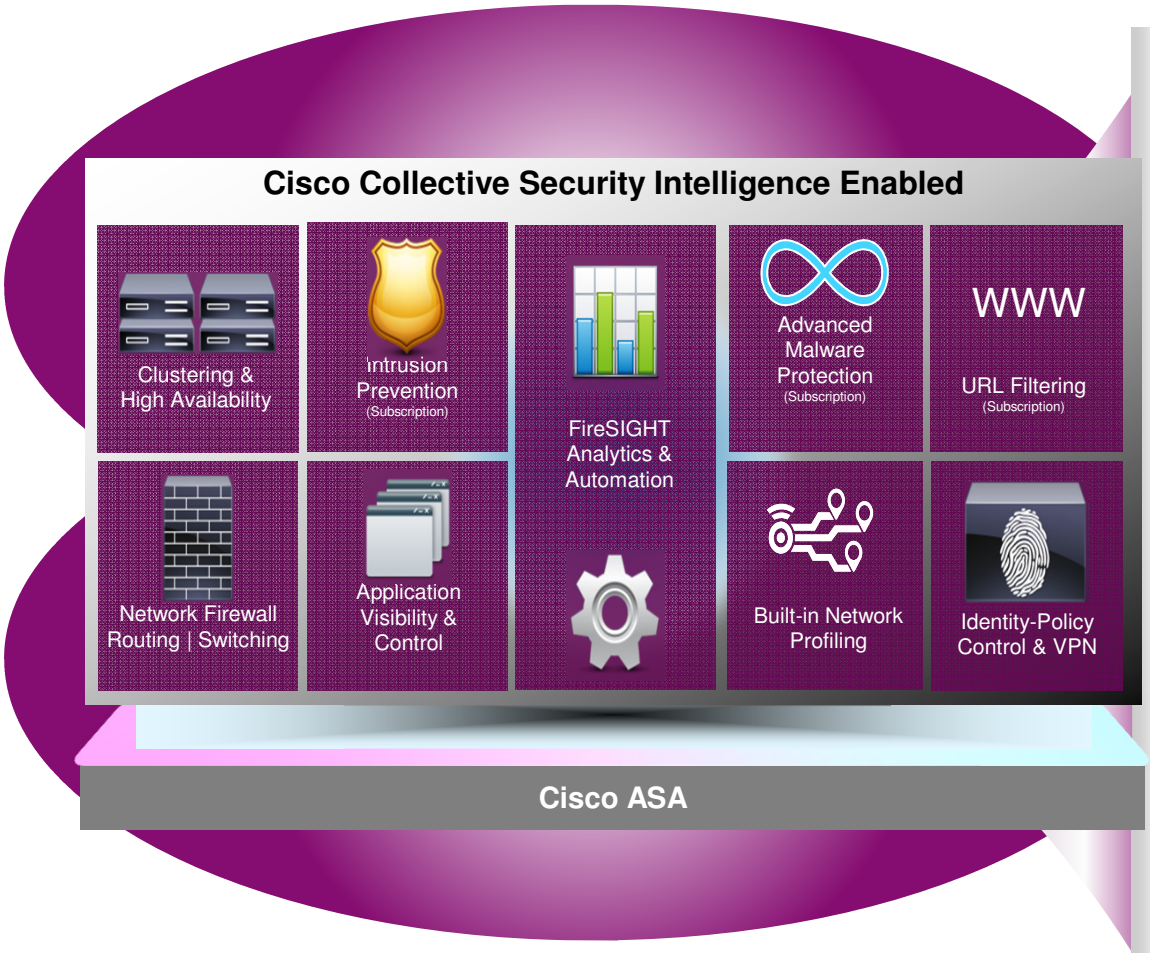
MDM Integration

airwatch™
CITRIX®
ZENPRISE Put Mobile to Work
Good
SAP
IBM
MobileIron

Corporate and Personal Device Posture Check and MDM Remediation

C97-726694-00 © 2013 Cisco and/or its affiliates. All rights reserved.

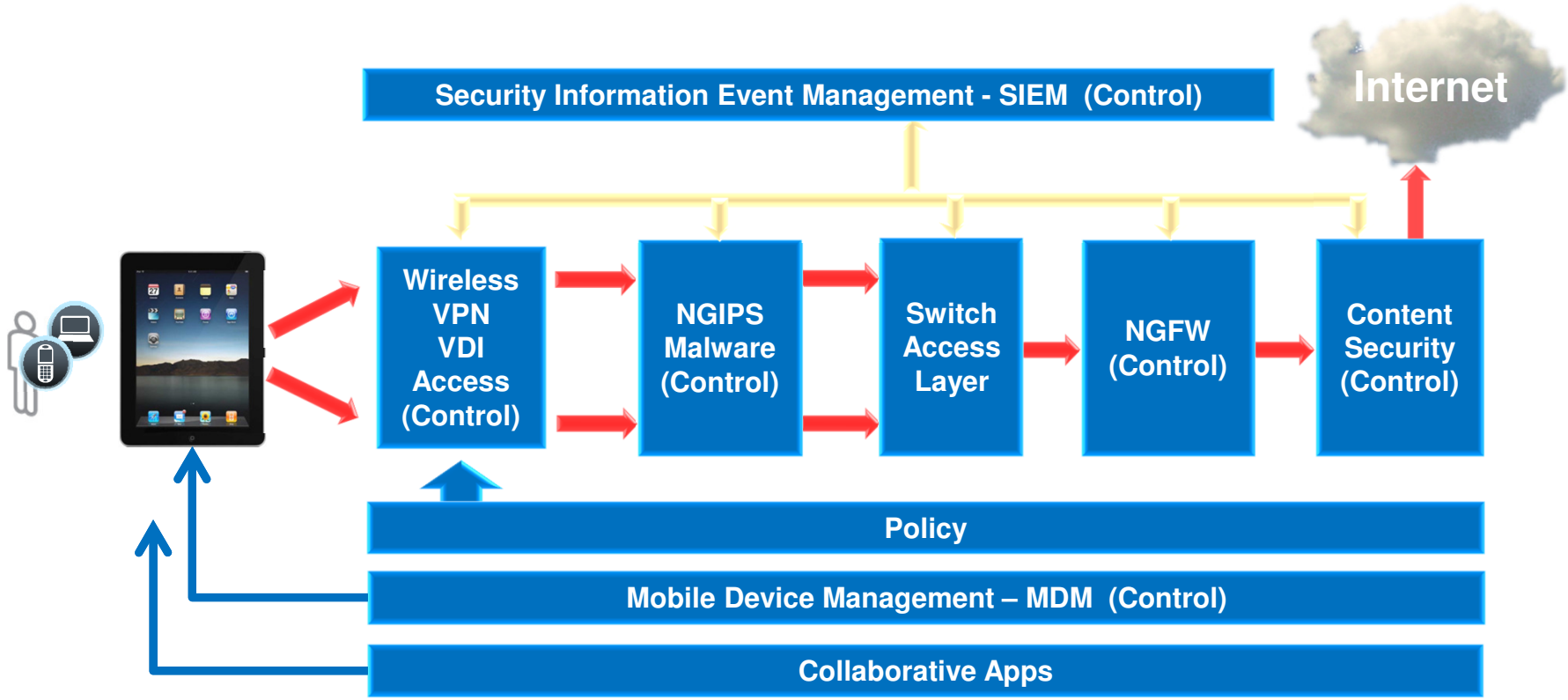
MULTI-LAYERED ATTACK PROTECTION



- World's most widely deployed, enterprise-class ASA stateful firewall
- Granular Cisco® Application Visibility and Control (AVC)
- Industry-leading FirePOWER next-generation IPS (NGIPS)
- Reputation- and category-based URL filtering
- Advanced malware protection

PRESIDIO

Presidio BYOD Architecture



Mobile Device Management
- Device Management
- Selective/Full Wipe
- Security Enforcement
- Access Control
- Certificate Mgmt
- App Mgmt and Distribution
- Content Mgmt

Policy
- 802.1x Authentication
- Authorization
- Profiling
- Posture Assessment
- Remediation
- Guest Services
- Mobile Onboarding
- Reporting
- Network Visibility

NGIPS-Malware
- Malware/Spyware
- DDoS Attacks
- Reconnaissance Attacks

SIEM
- Logging
- Correlation
- Reporting

NG-Firewall
- Access Control
- Remote Access VPN
- Dynamic Access Policies

Content Security
- Email/Web Defense
- Data Security
- Acceptable Use

Collaborative Apps
- Voice
- Video
- Instant Messaging
- Presence
- * VXI

BYOD AND MOBILE SECURITY ASSESSMENT

BYOD Mobile Use-Case Assessment

- Infrastructure Survey
- Application Delivery Survey
- BYOD Mobile Requirements

Mobile Security Assessment

- Mobile Security Policies
- Perimeter Security
  - Firewall
  - Remote Access
  - IPS and Malware Protection
  - MDM
  - Content Security
  - Application Management
- Network Security
  - LAN/WAN
  - Wireless
- Security Monitoring

When?

- Developing a BYOD Strategy
- Embarking on a BYOD Initiative

Executive Summary Report

Detailed Technical Report

Plan of Action and Milestones

Why?

- Identify vulnerabilities in BYOD architecture
- Provide a BYOD strategy, guidelines, policies and architecture

PRESIDIO

NEXT STEPS

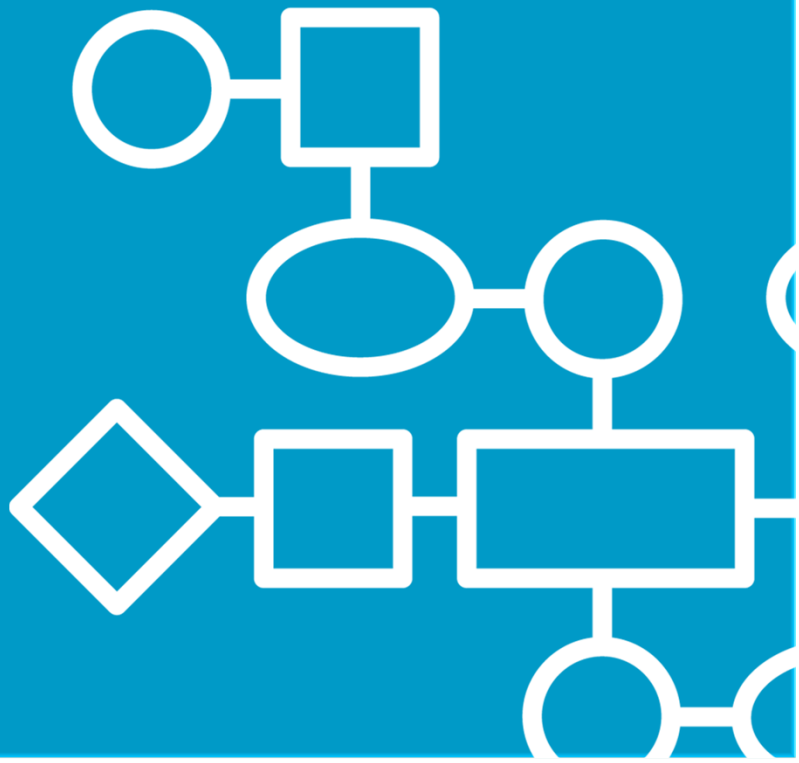
Evaluate Software
- Policy/NAC
- NGFW
- NG-IPS
- MDM
- Content Security
- Malware
- SIEM

Policy Development

BYOD Assessment

PRESIDIO™

Practical thinking for a connected world.



THANK YOU.