Best Practices for Securing Mobile Content

Ojas Rege, *VP Strategy*, MobileIron

Professional Techniques – T13

ISACA®
Trust in, and value from, information systems
San Francisco Chapter
2014 Fall Conference - "Think Big"
CRISC
CGEIT
CISM
CISA

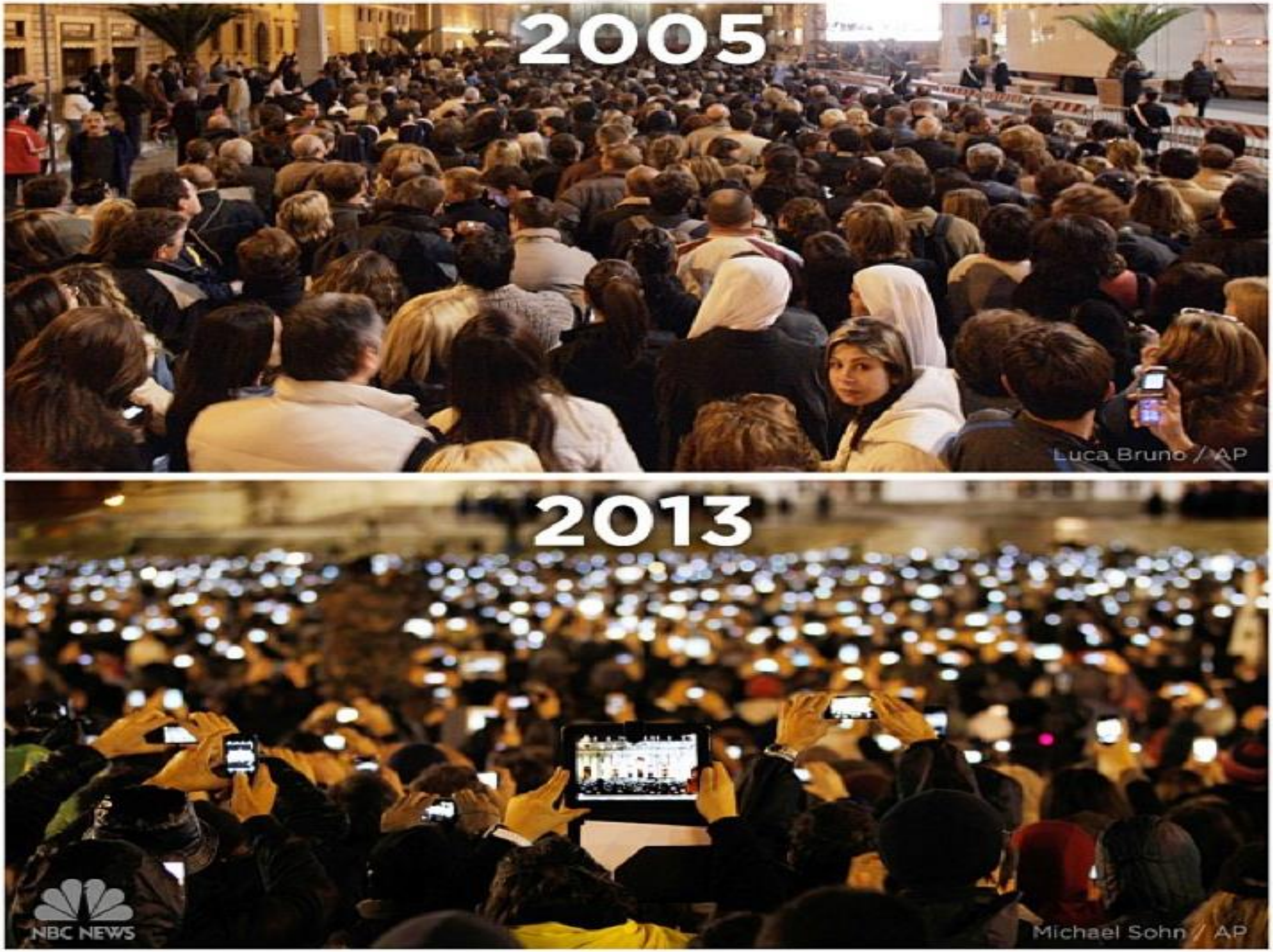
Today's session

Objectives

- Establish the link between mobile and content
- Outline the security considerations for mobile content
- Share best practices for content security

Agenda

- What is Mobile First?
- Content security use cases
- Baseline best practices
- Hacker threats and countermeasures
- Evolution of security model



2005

Luca Bruno / AP

2013

Michael Sohn / AP

Kaffee 4,5m WAL

MOBILE FIRST

Definition…

Mobile First organizations embrace mobility as their primary IT platform in order to transform their businesses and increase their competitiveness.

In a Mobile First Company…

APPLICATIONS

New apps are developed and delivered to mobile devices first

Core business processes can be performed on any device

CONTENT

Content of all types is easily and securely available on any device

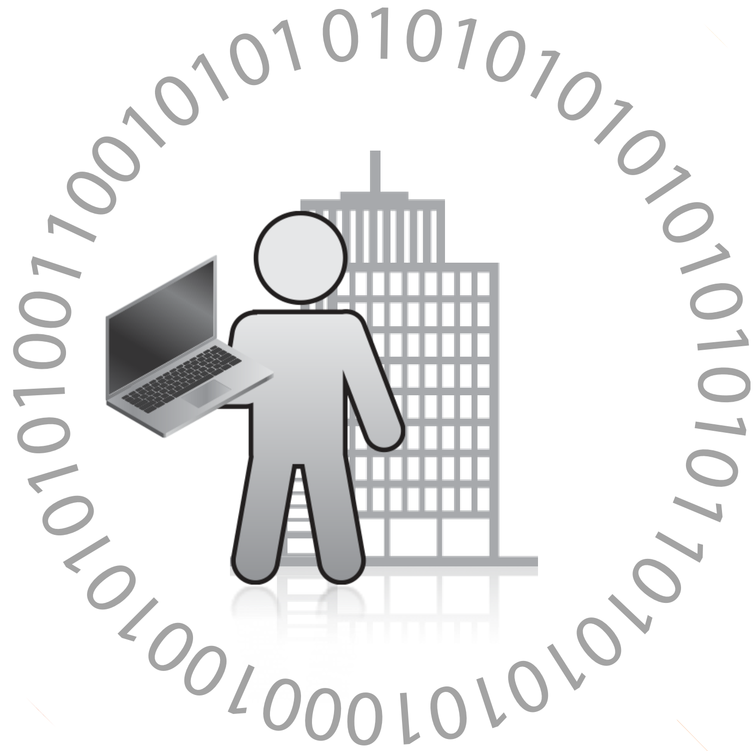
USER EXPERIENCES

End users choose their devices

Security is invisible to end users

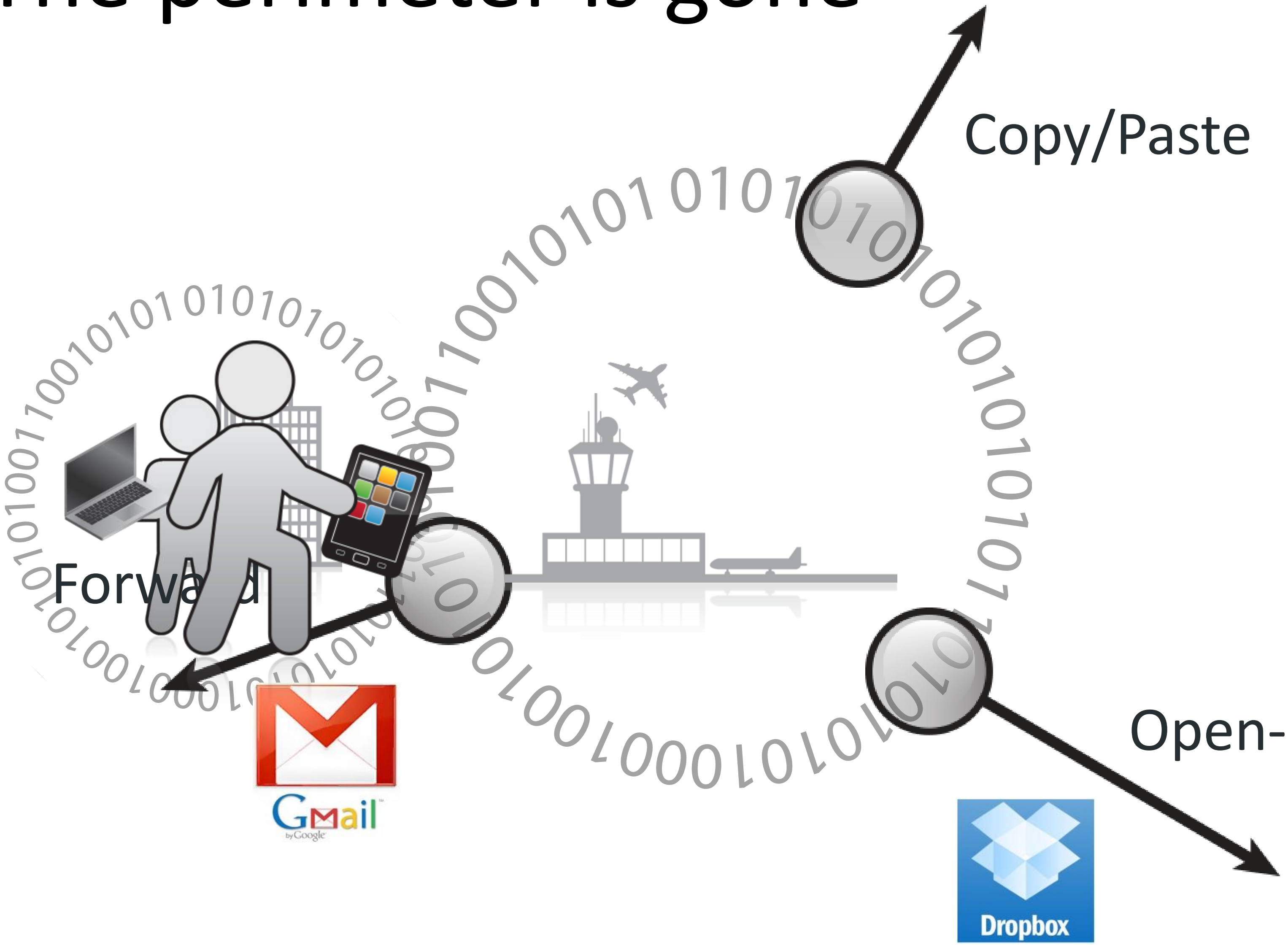
User experience is the #1 design criteria

Traditional enterprise security



Firewall
& VPN

The perimeter is gone



Copy/Paste

Forward

Open-in

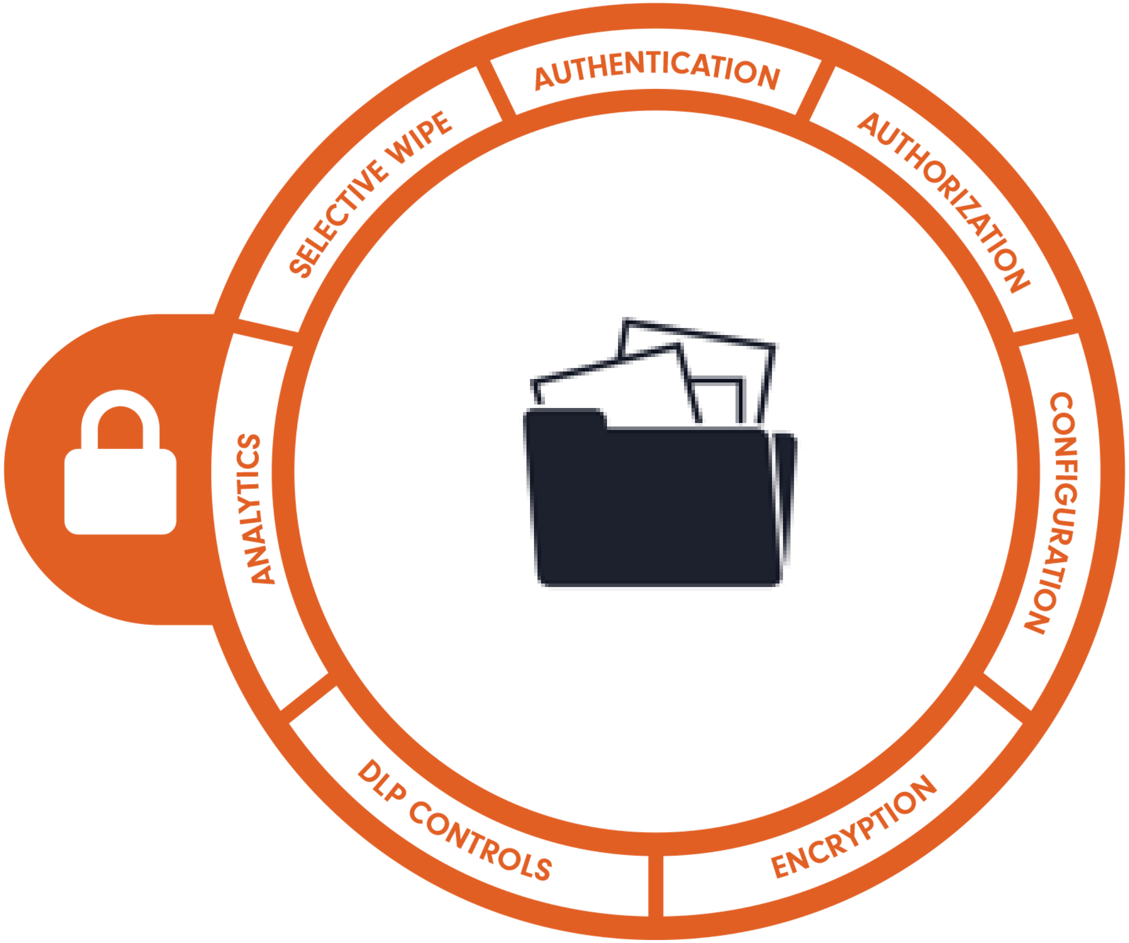
“The more the CIO says ‘No,’ the less secure the organization becomes.”

Vivek Kundra
CIO, United States, February 2011

“Responsible, not restrictive.”

Mike Brannon
National Gypsum

Securing data-at-rest



Two primary document repositories

Email attachments

View **Save**

Copy **Open In**

SharePoint documents

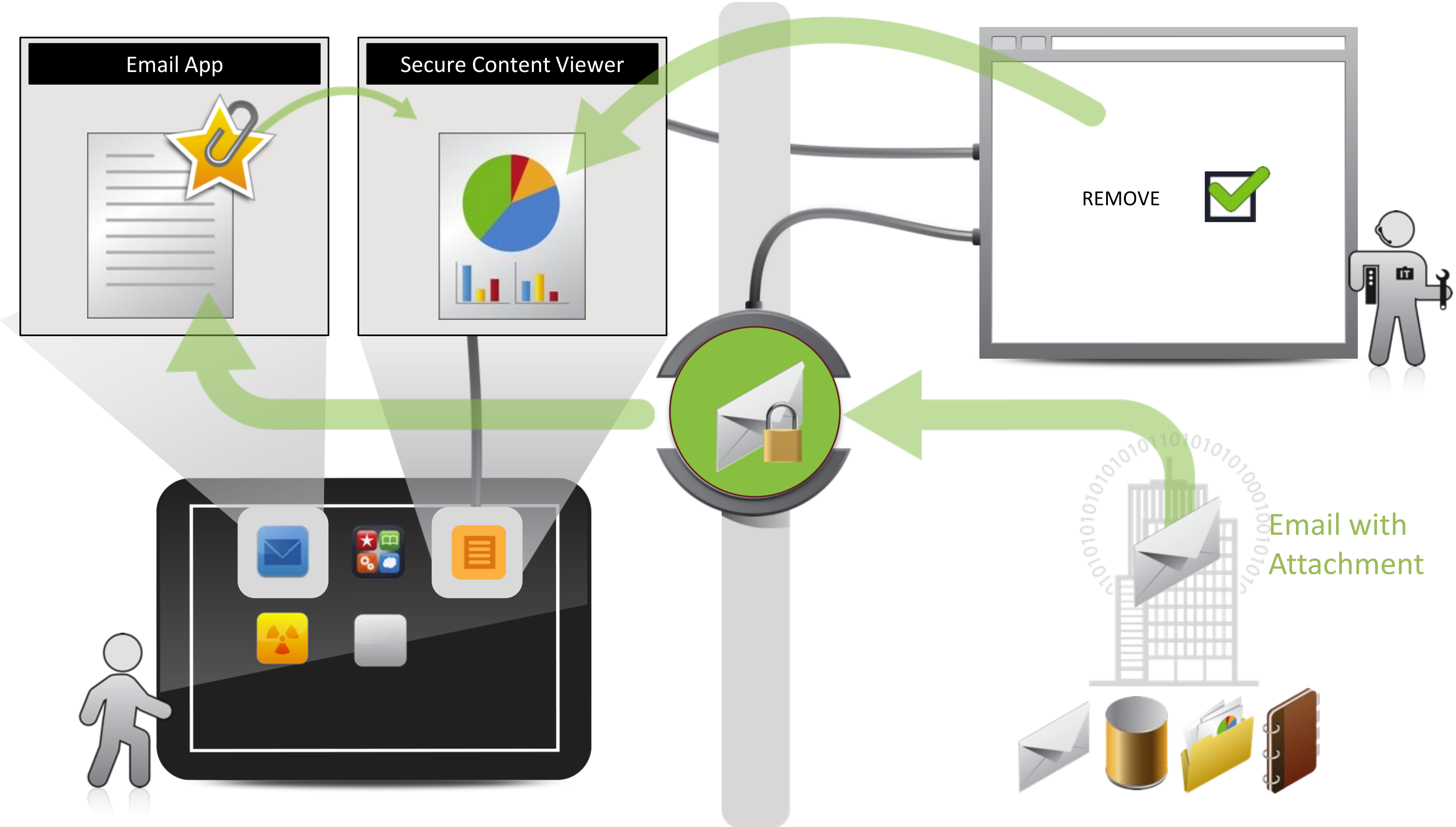
View **Save**

Copy **Open In**

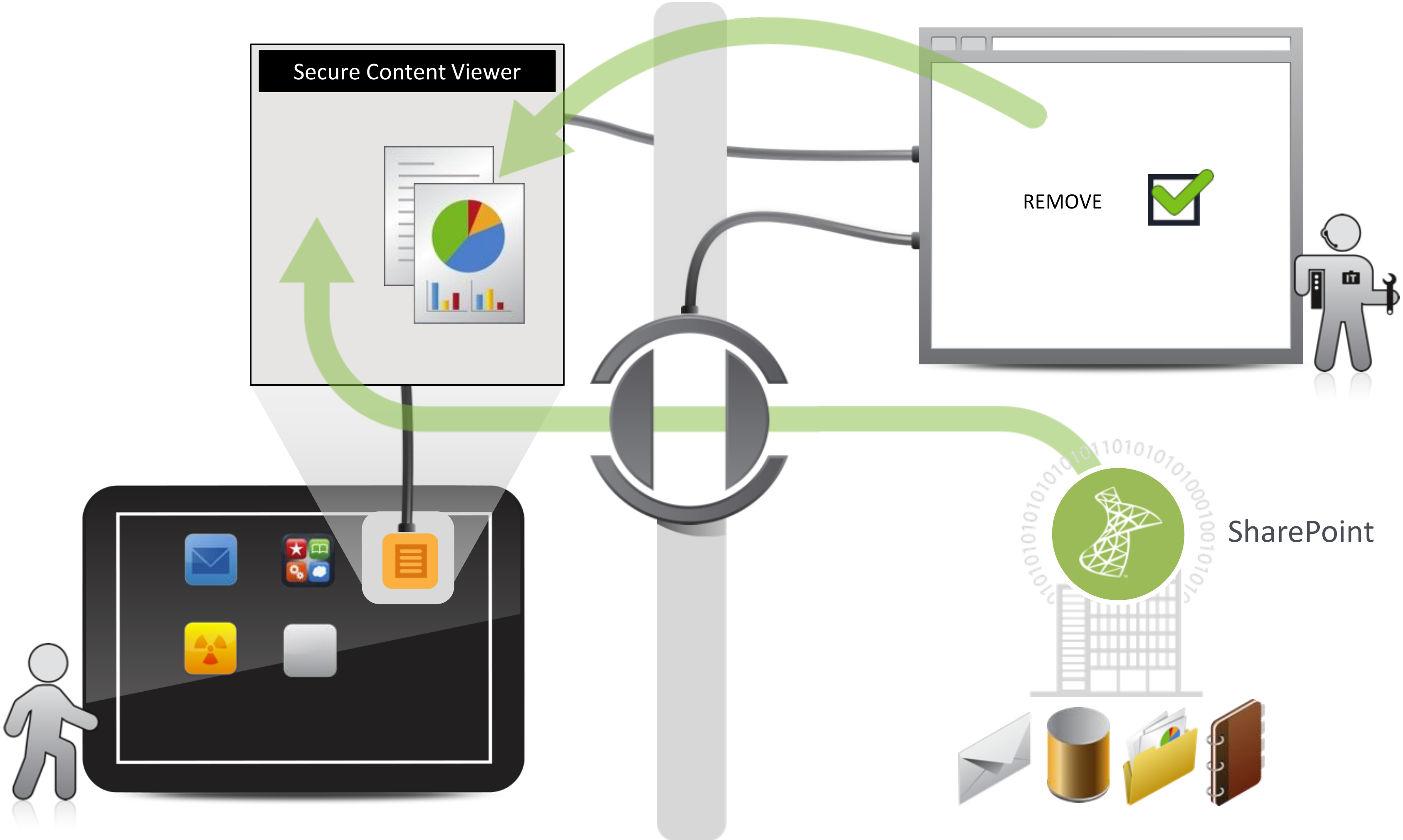
- Solve “**open in**” problem
- Store documents securely on device
- Control cut / copy / paste actions
- Selectively wipe documents
- Prevent unauthorized distribution

- Control end-to-end with policy
- Leverage existing content repositories

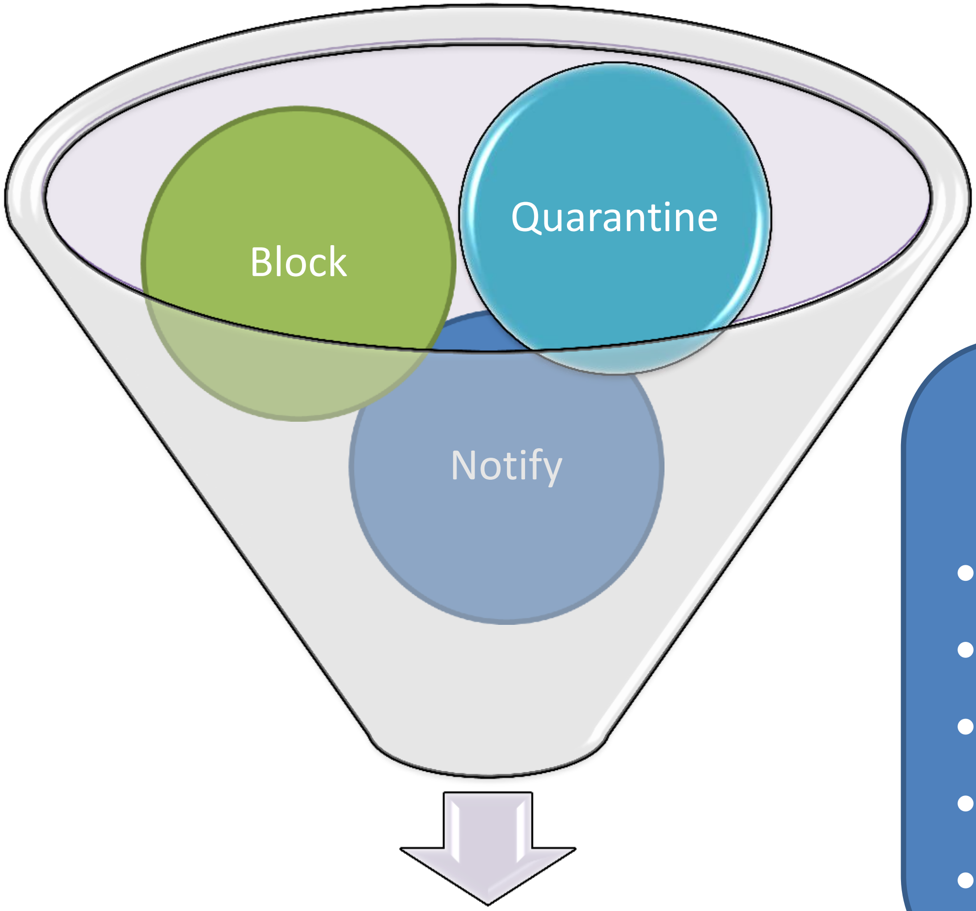
Securing email attachments



Securing SharePoint



Closed loop actions when compromised

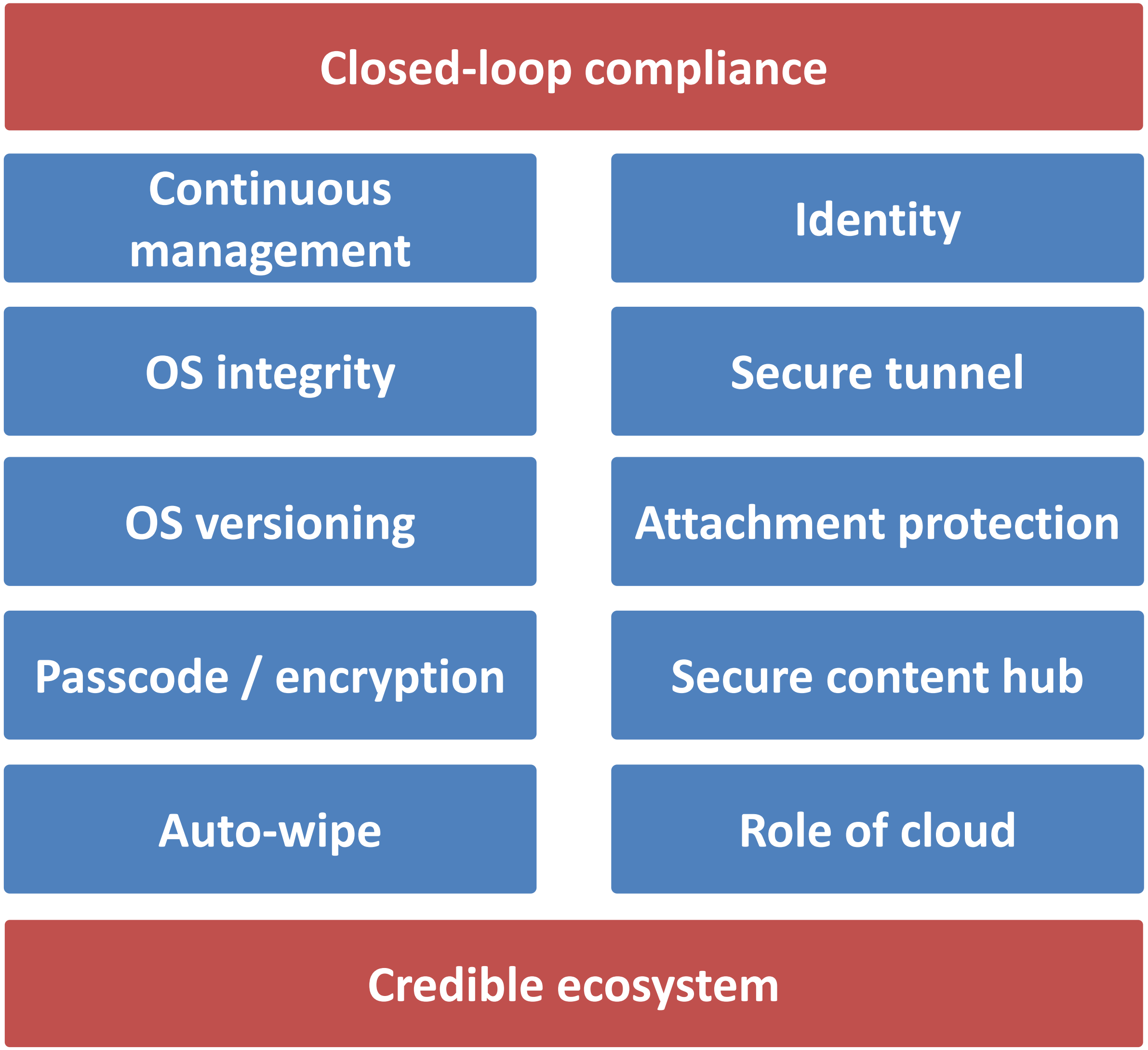


Remediation

Closed-loop actions

- Notify user and admin
- Prevent access
- Remove saved files
- Remove SharePoint config
- Protect enterprise persona

Best practices for data loss prevention



Closed-loop compliance

Continuous management

Identity

OS integrity

Secure tunnel

OS versioning

Attachment protection

Passcode / encryption

Secure content hub

Auto-wipe

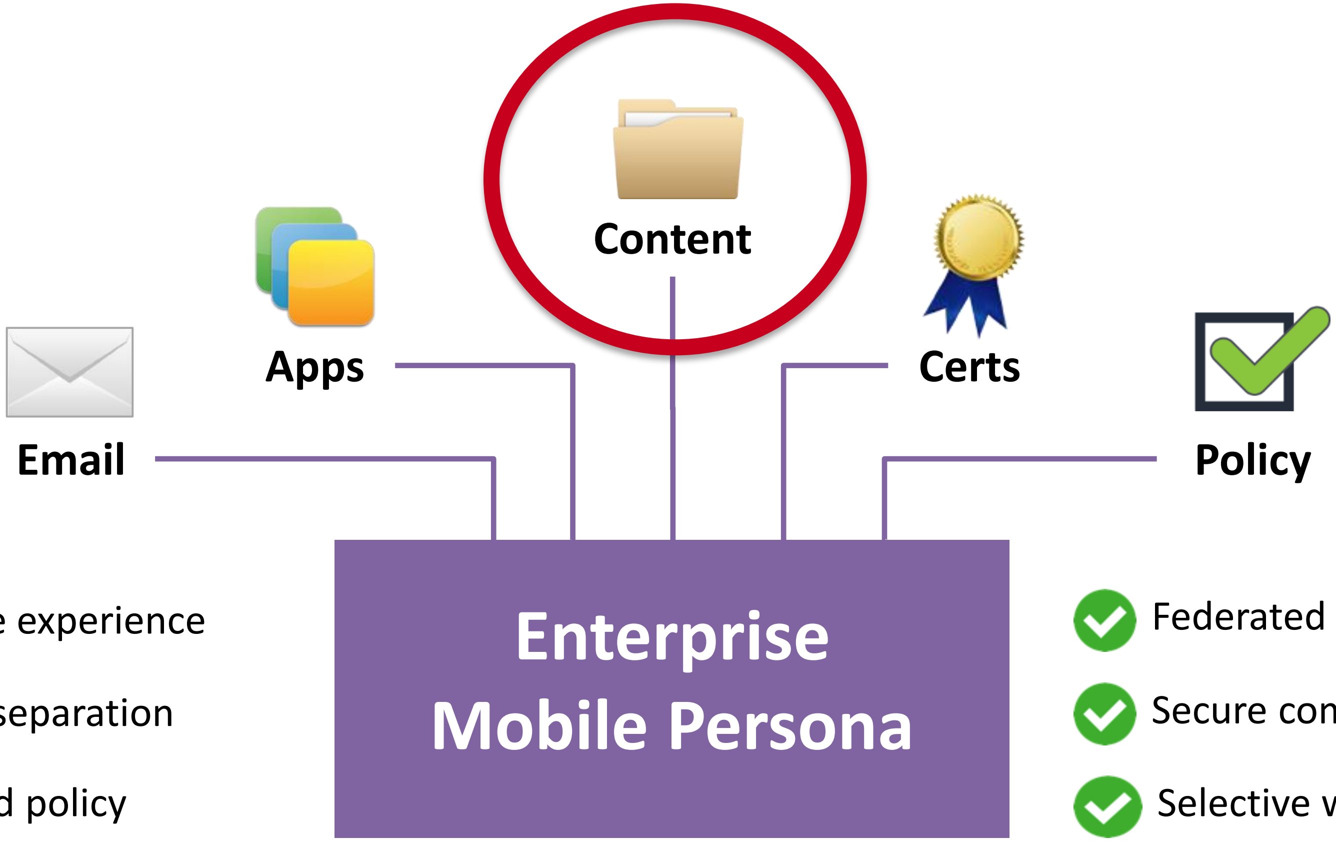
Role of cloud

Credible ecosystem

Security considerations 2014+

- Content always one-click from cloud -> co-habitate responsibly
- “No” not a sustainable option -> provide credible alternatives
- Massive content ecosystem -> crowd-source but don’t lock-in
- Dynamic risk at endpoint -> automate your mobile trust model
- Uncertain economics -> establish “help-yourself-desk”
- Blurring between content and app -> explore new forms

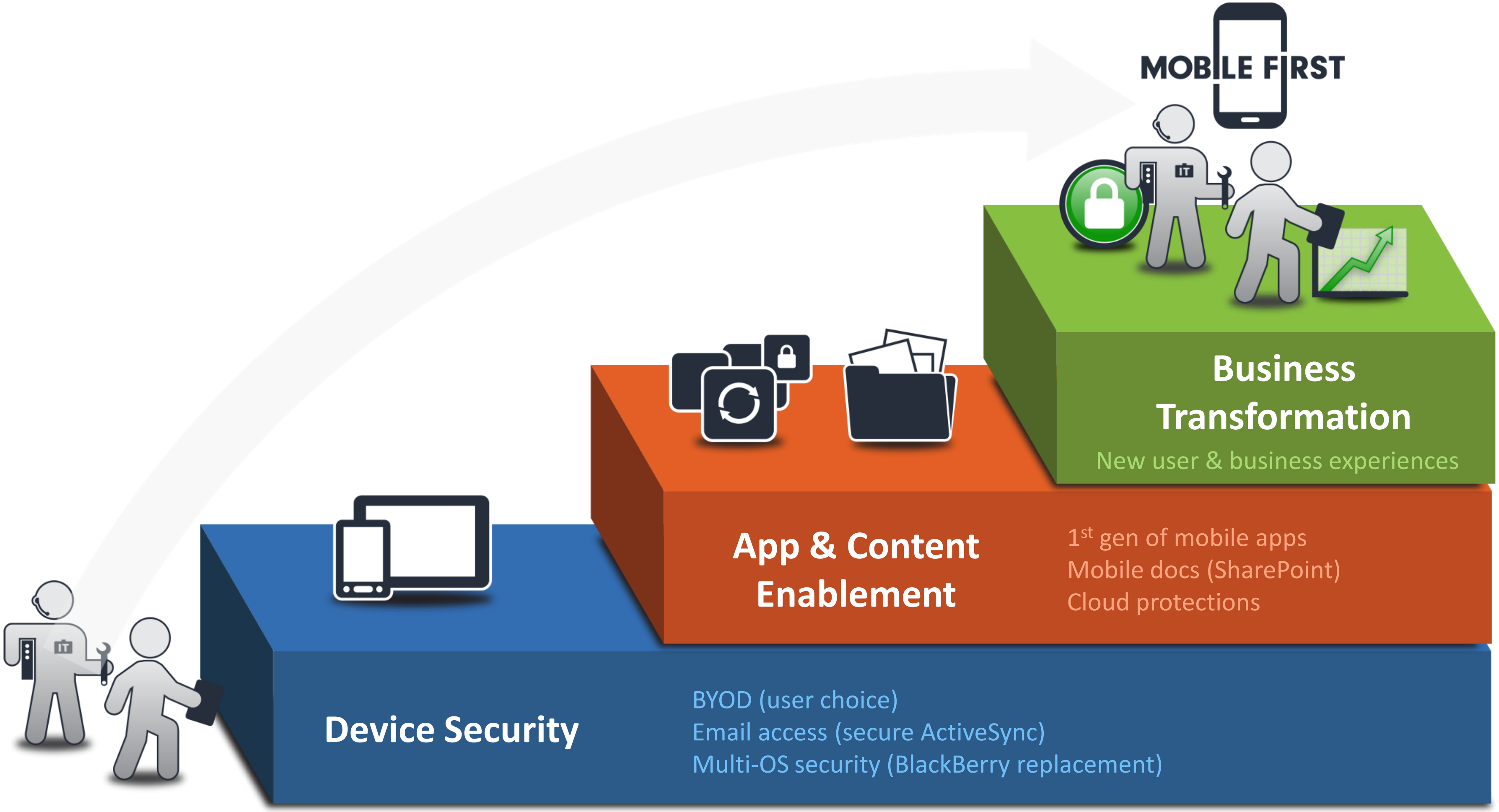
Content does not exist in isolation



- ✓ Native experience
- ✓ Data separation
- ✓ Shared policy

- ✓ Federated identity
- ✓ Secure communications
- ✓ Selective wipe

Journey to the Mobile First enterprise



Business Transformation

New user & business experiences

App & Content Enablement

1st gen of mobile apps
Mobile docs (SharePoint)
Cloud protections

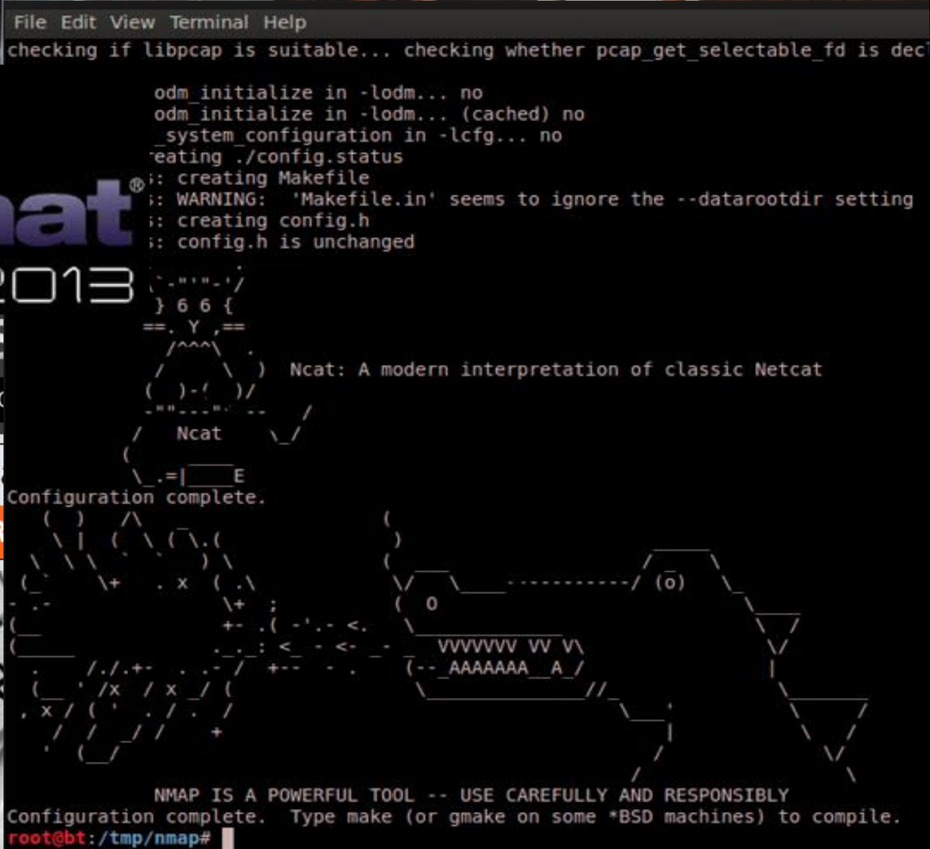
Device Security

BYOD (user choice)
Email access (secure ActiveSync)
Multi-OS security (BlackBerry replacement)

Hacker culture

black hat® USA 2013

dc404



```
checking if libpcap is suitable... checking whether pcap_get_selectable_fd is decl

odm_initialize in -lodm... no
odm_initialize in -lodm... (cached) no
_system_configuration in -lcfg... no
reating ./config.status
: creating Makefile
: WARNING:  'Makefile.in' seems to ignore the --datarootdir setting
: creating config.h
: config.h is unchanged

        Ncat: A modern interpretation of classic Netcat

    Ncat

Configuration complete.

     NMAP IS A POWERFUL TOOL -- USE CAREFULLY AND RESPONSIBLY
Configuration complete.  Type make (or gmake on some *BSD machines) to compile.
root@bt:/tmp/nmap#
```

Motivations

Joining the "elite"

- Show technical prowess
- Publish that exploit first

A poke in the eye of bureaucracy

- "Big Business"
- "Big Government"

Criminal intent

- Corporate espionage
- Money or credit card numbers

Payback for wrong deed

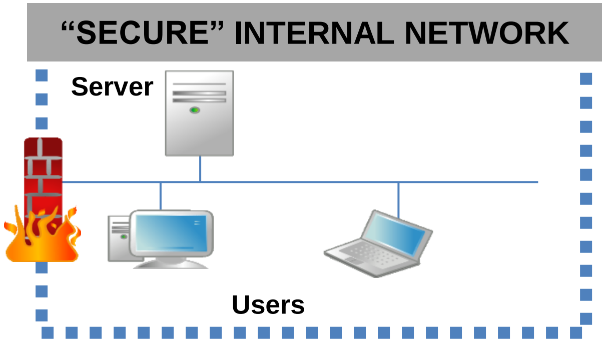
- Revenge!

Rule the world!

World has changed – for IT and hacker

New gen operating systems are sandboxed

Network edge has blurred



User is low-hanging fruit

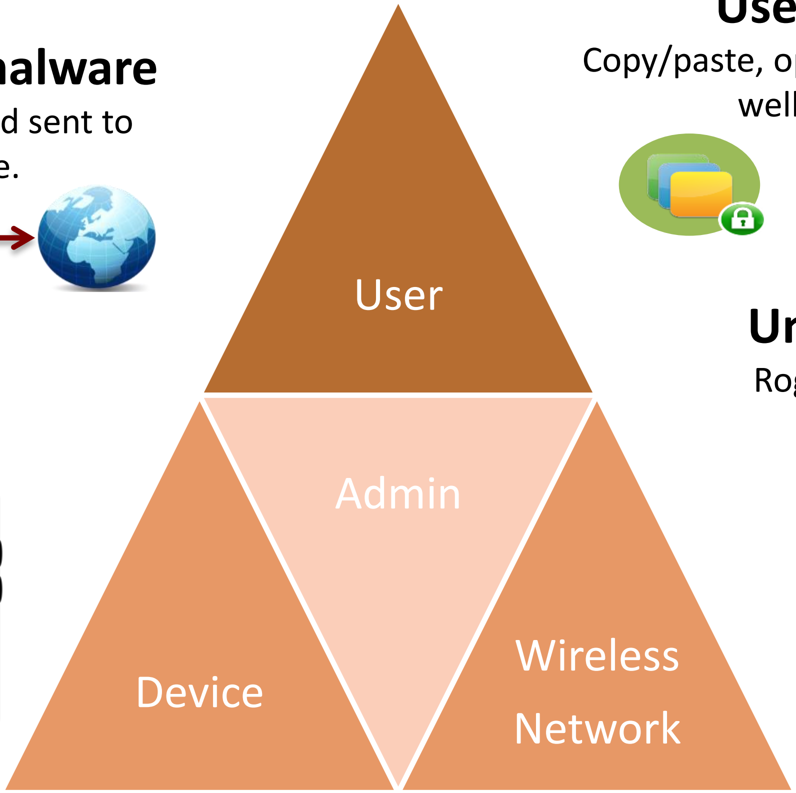
Mobile attack vectors

Spyware and malware

Data is harvested and sent to malicious site.

Jailbreak / root

Device is opened to vulnerabilities leading to data exposure.

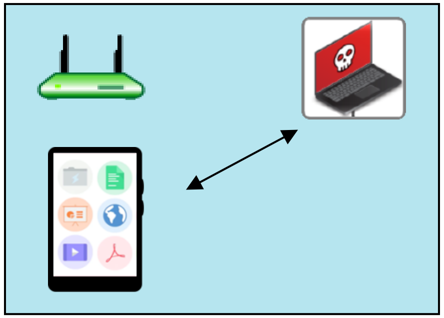


User data leakage

Copy/paste, open in, etc. lead to leaks from well-intentioned users.

Unprotected networks

Rogue access point, man-in-the-middle, etc. capture data.

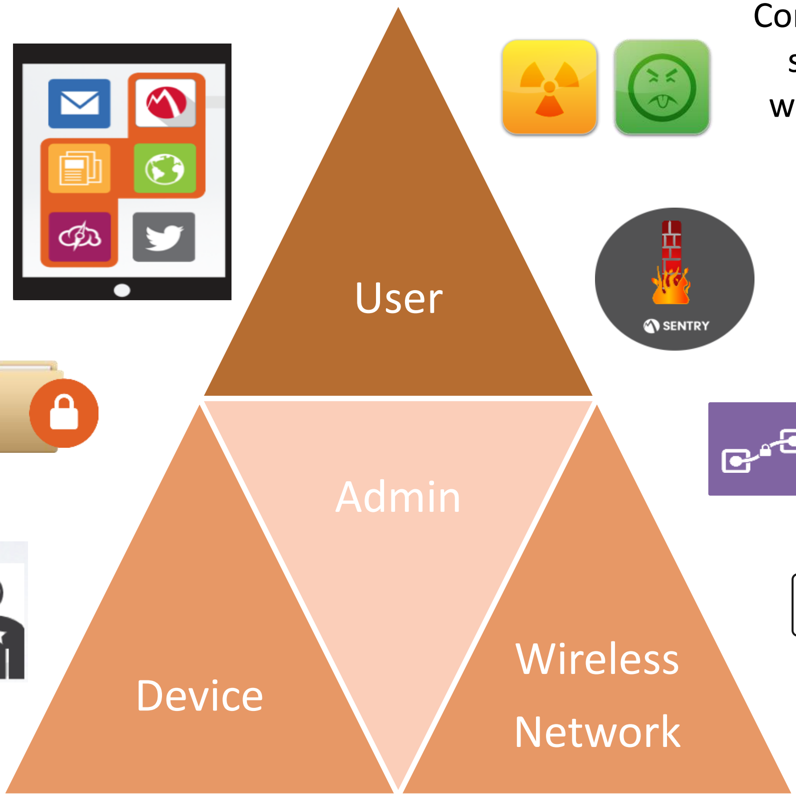


Countermeasures framework

Data loss prevention (DLP) controls mitigate device vulnerabilities and prevent well-intentioned users from leaking corporate data.

Secure email attachments enforce DLP and mitigate device vulnerabilities.

Quarantine of jailbroken and rooted devices (online & offline) prevent ongoing threat.



Containerization and app reputation services protect against risky apps without unnecessary limitations on app downloads.

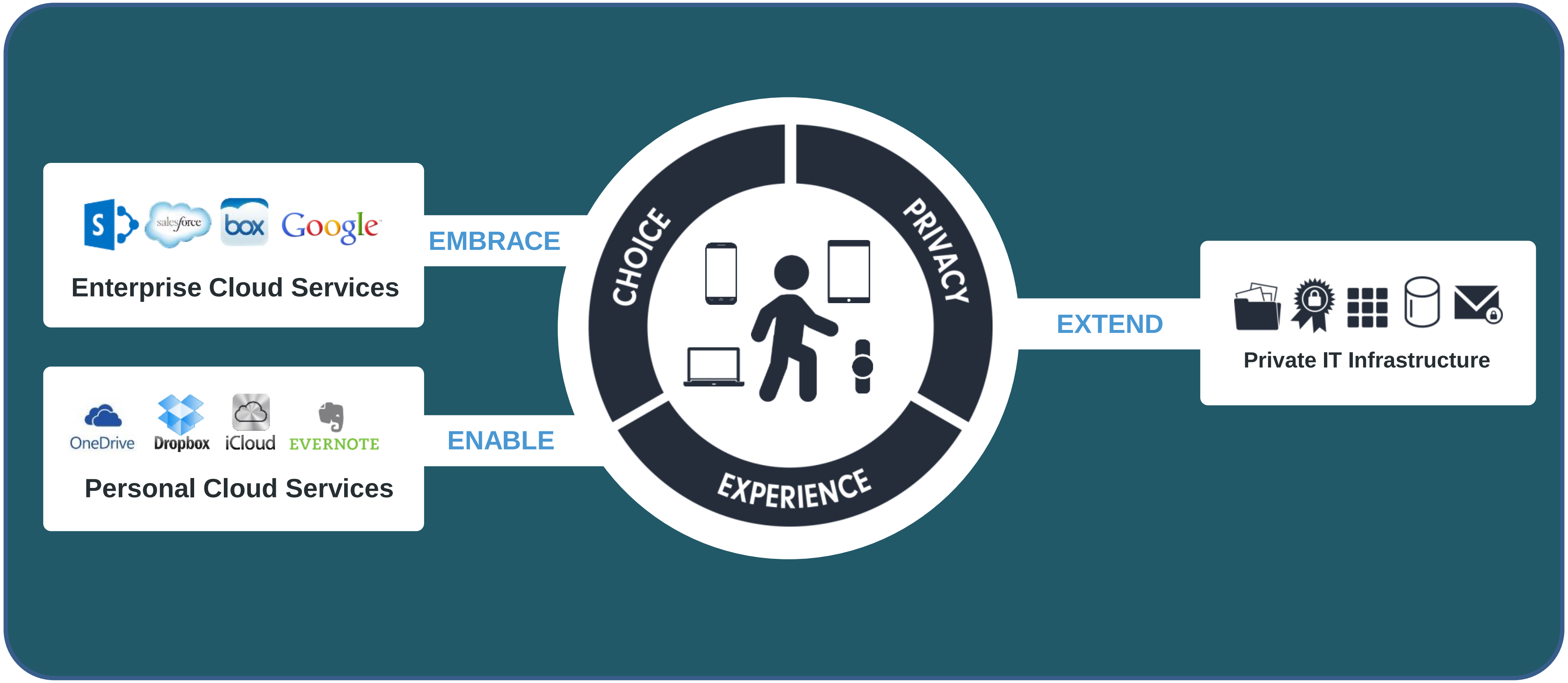
Sentry gateway prevents unauthorized devices and apps from gaining access.

Secure, isolated tunnel separates and protects work app traffic.

Certificates thwart open Wi-Fi MiTM attacks.

Ensures appropriate cryptographic use.

The new enterprise IT architecture



Enterprise Cloud Services

EMBRACE

Personal Cloud Services

ENABLE

CHOICE

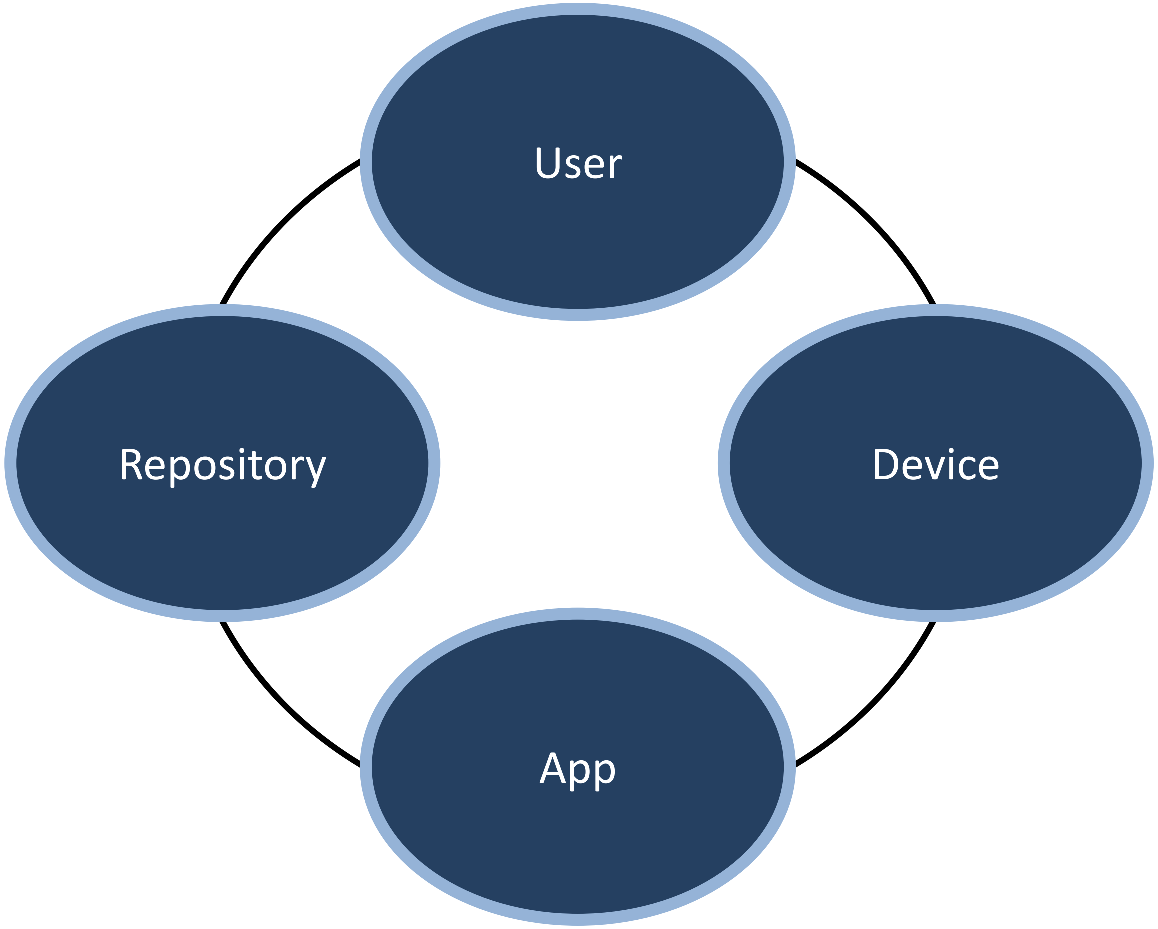
PRIVACY

EXPERIENCE

EXTEND

Private IT Infrastructure

Circle of trust



User

Device

App

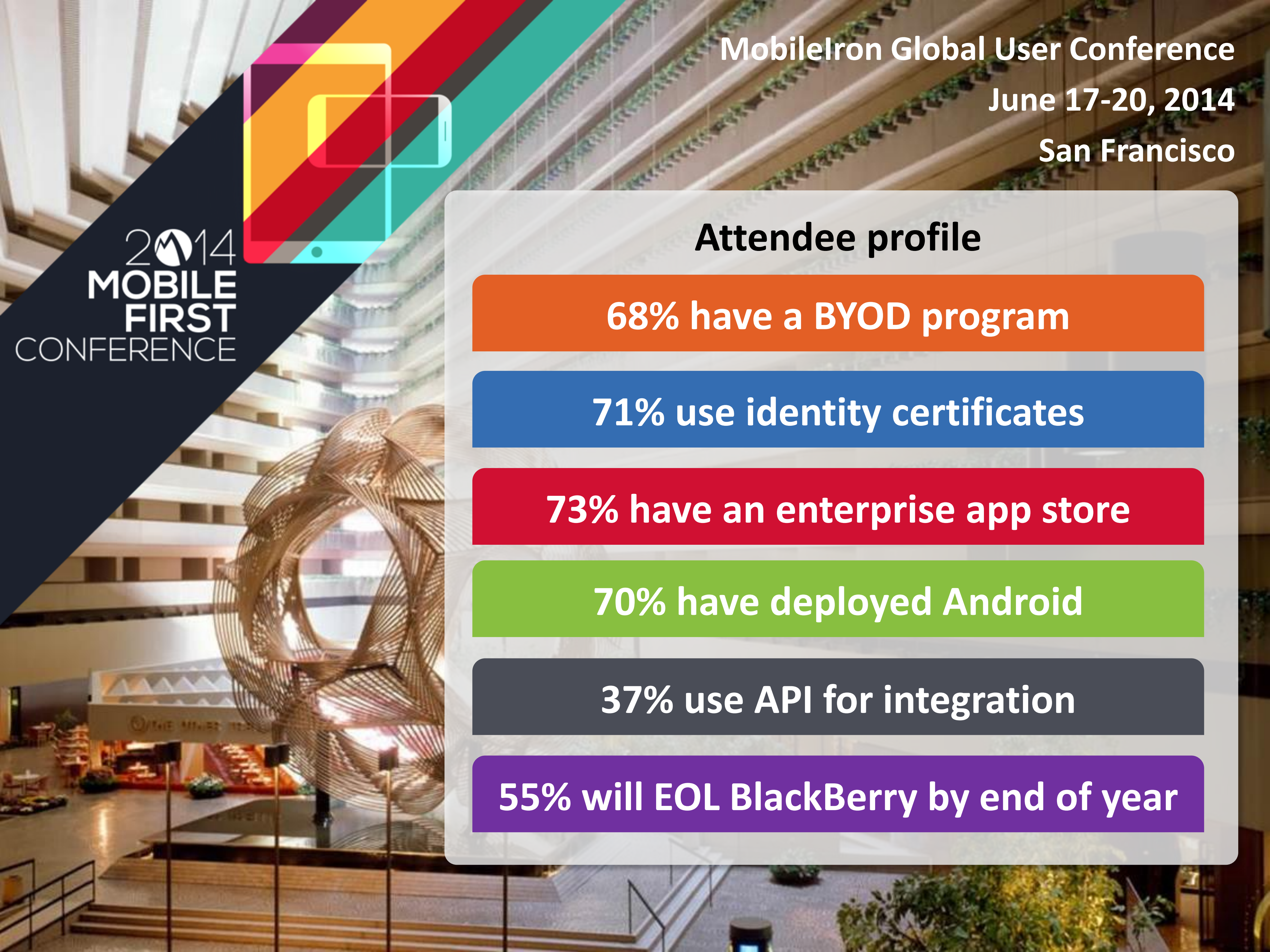
Repository

Evolution of IT: Agility is the new security

What factors would most contribute to your organization's ability to maintain an effective mobile strategy over time?

Source: Ponemon Institute, March 2014

Most important factors for mobile success *(7 = most important to 1 = least important)*	
Agility and preparedness for change	**6.58**
Ample resources	6.01
Enabling technologies	5.60
Knowledgeable or expert staff	5.13
Collaboration among business units	4.24
Effective leadership	3.97
A strong mobile security posture	2.61



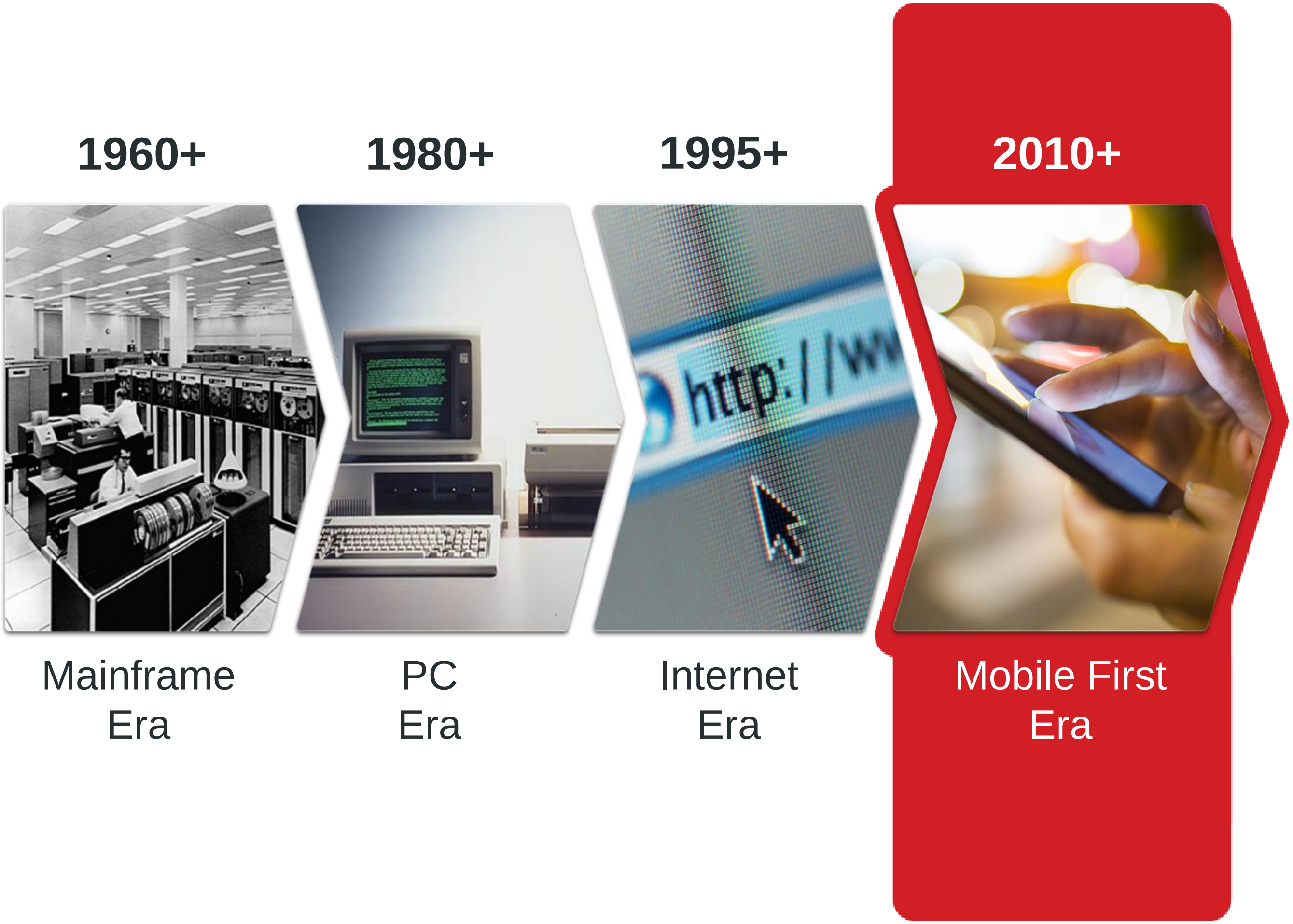
2014 MOBILE FIRST CONFERENCE

MobileIron Global User Conference
June 17-20, 2014
San Francisco

Attendee profile

- 68% have a BYOD program
- 71% use identity certificates
- 73% have an enterprise app store
- 70% have deployed Android
- 37% use API for integration
- 55% will EOL BlackBerry by end of year

Major technology and business transition



1960+ Mainframe Era

1980+ PC Era

1995+ Internet Era

2010+ Mobile First Era

Past technology transitions

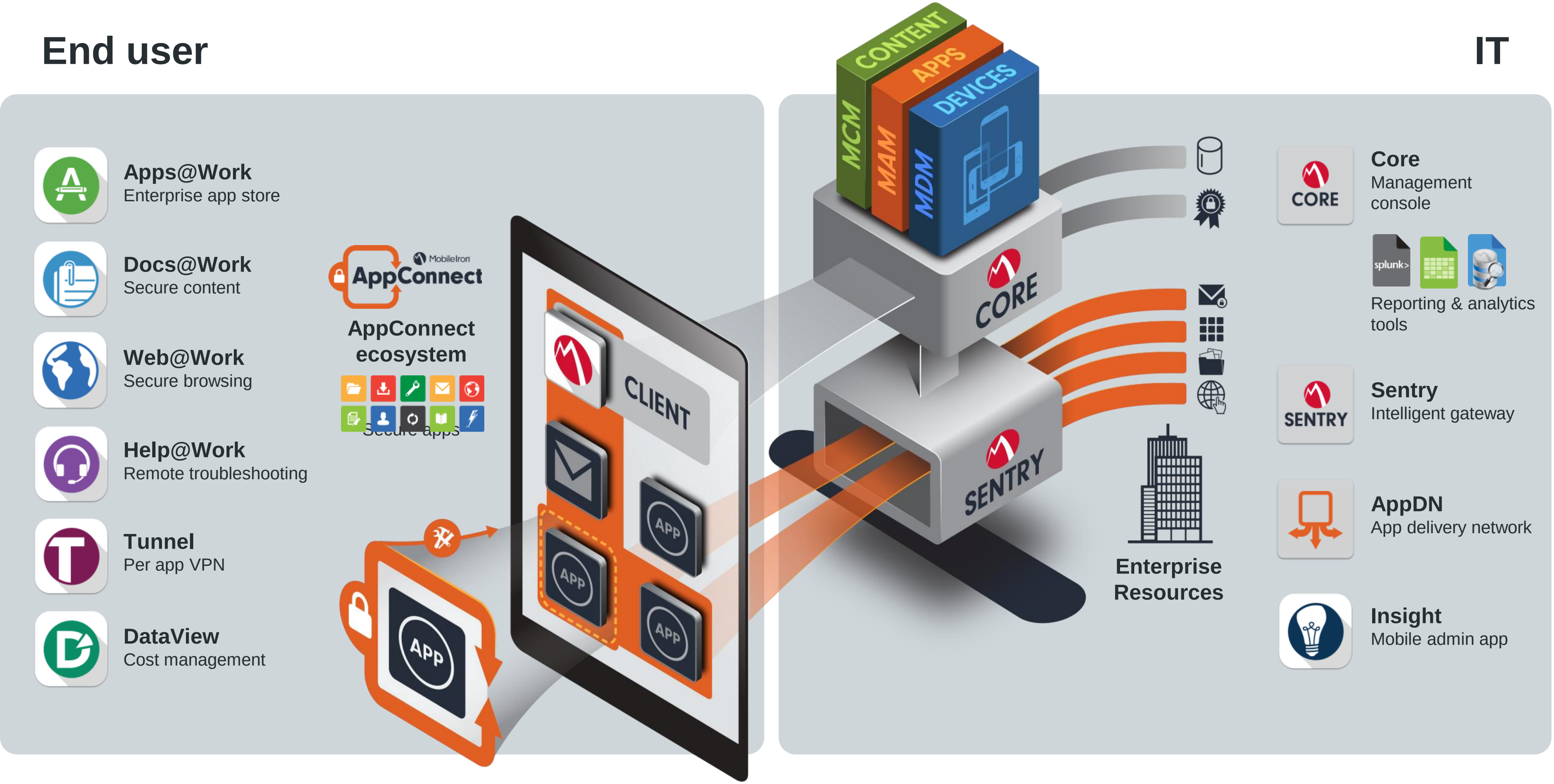
- Change the way people work
- Disrupt enterprise architectures
- Create opportunities for innovation

MobileIron®

MOBILE FIRST

Mobility unlocks human potential in the workplace

MobileIron: Purpose-built architecture for enterprise security and management



End user

Apps@Work
Enterprise app store

Docs@Work
Secure content

Web@Work
Secure browsing

Help@Work
Remote troubleshooting

Tunnel
Per app VPN

DataView
Cost management

AppConnect ecosystem
Secure apps

IT

Core
Management console

Reporting & analytics tools

Sentry
Intelligent gateway

AppDN
App delivery network

Insight
Mobile admin app

Enterprise Resources

Thank you!

Ojas Rege
ojas@mobileiron.com
@orege (twitter)