

# Mobile App Security and Malware in Mobile Platform

**Siupan Chan**

Sales Engineering Manager, Greater China

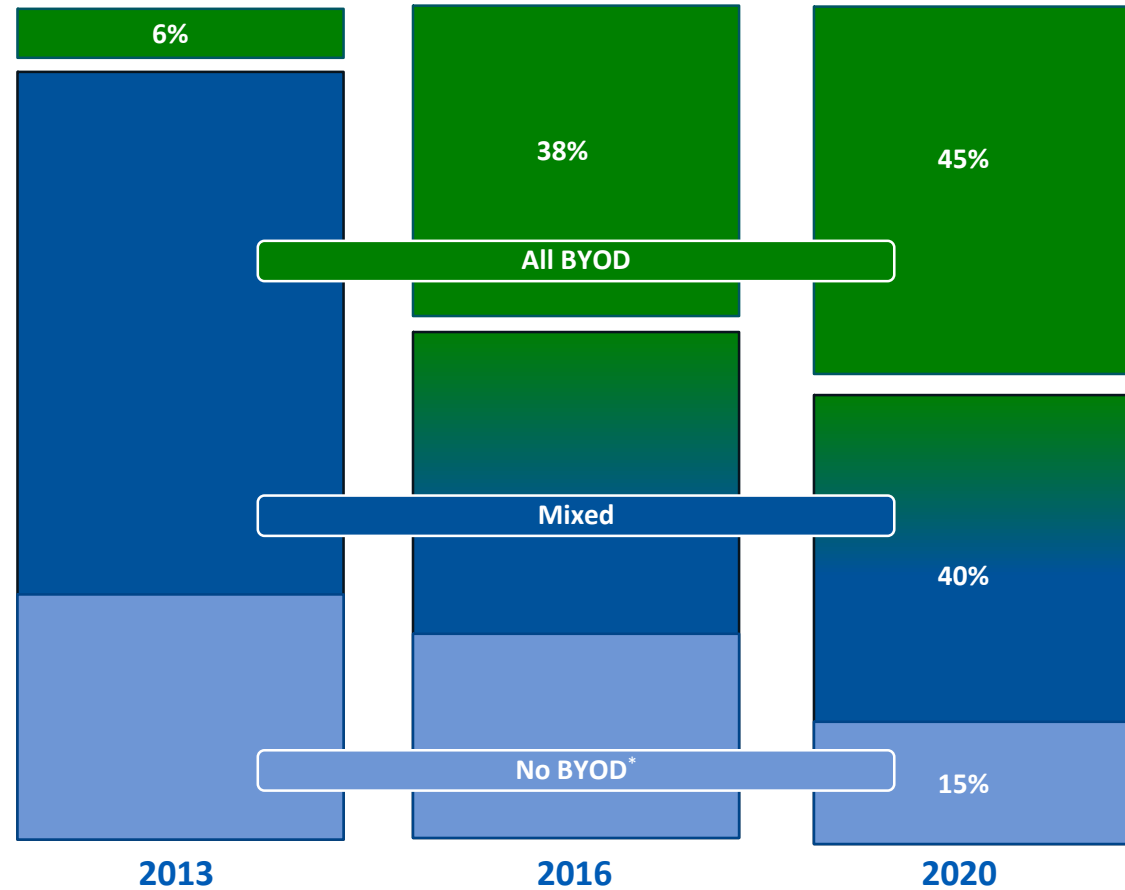
23 September, 2016

**SOPHOS**

# The Mobile Security Epidemic

# A Radical Shift is Occurring

*“When will your organization cease to provide personal devices?”*



\*Source: Bring Your Own Device: The Facts and the Future, 2013  
n=2053 CIOs, worldwide

# Trends

## Security or data breaches involving mobile devices are on the rise

2x

Data breaches involving smartphones or tablets more than **doubled** in 2015 <sup>(1)</sup>

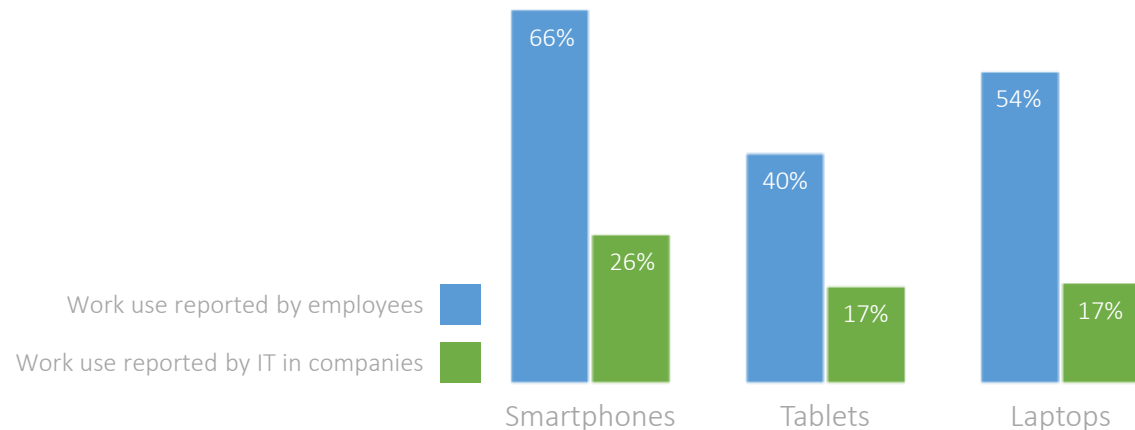
15%

of large organizations have had a security or data breach involving smartphones or tablets in 2015 <sup>(1)</sup>

## More people use mobile devices for work than their companies think

2/3

of employees say they use their **personal** smartphones for work; their companies think only **25%** do... <sup>(2)</sup>



# Productivity/Management vs Security

**Provide services while balancing both**



- Secure the data
- Protect the customers
- Protect the users
- Protect the business

- Just let me do my job
- No training required
- Ease of use
- Access data on demand



# Malware Goes Mobile: Timeline of Mobile Threats, 2004 – 2015

2004



**Cabir**

First worm affecting Symbian Series 60 phones. Spreads from phone to phone by using Bluetooth OBEX push protocol.

**Ikee and Duh**

Worms affecting jail-broken iPhones using Cydia app distribution system due to a hard-coded password in sshd.

2010



**FakePlayer**

First malware for Android makes money by sending SMS messages to premium line numbers in Russia.

**DroidDream**

First large attack on Google Play. Over 50 apps containing a root exploit published on the Android market.



2011

2012



**Zitmo**

Popular Windows bot and banking malware Zeus improved with its Android component designed to steal mobile transaction authentication numbers (mTANs).

**Masterkey**

A vulnerability in Android exploiting certificate validation, allowing malware to disguise itself as a legitimate app.

1000 new Android malware samples discovered every day.



2013

2014



**DownAPK**

Windows based malware uses Android debugging bridge to install fake banking app to Android devices connected to the infected PC.

2000 new Android malware samples discovered every day.

**Gazon**

Android virus spams all your contacts via SMS with a link to install a phony Amazon rewards app.

2 million cumulative samples of Android malware and potentially unwanted apps.



2015

**SOPHOS**  
Security made simple.

# The Android Security Challenge

*According to Sophos Labs,*

During the years **2010-2014**, we have collected **1.1 million** unique samples of malware



For **2014**, we've identified about **500,000 new** unique pieces of malware



And another **500,000** unique **PUAs**

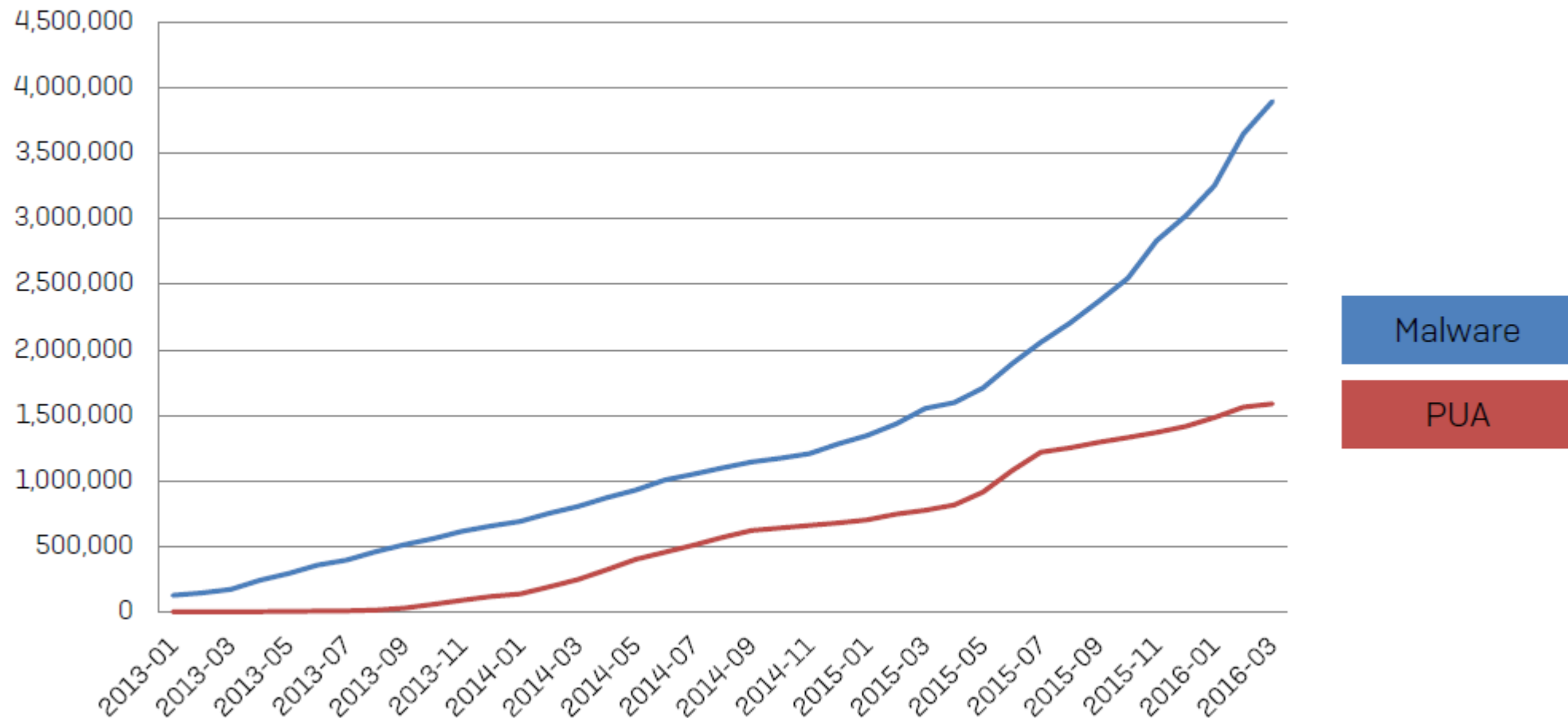


From **Sept 2013 – Sept 2014**, there was an **1800% increase** in malware



# Android Malware Growth

Android malware vs PUA growth - cumulative



Source: SophosLabs




# Phishing via SMS

Account notification: <http://yourbank.example.com>  
1 new Secure Email <http://mobile.bank.example>  
Your online statement is ready <http://m.bank.test/>



# Your location has been shared 5398 times

 Your location shared with 10 apps


Did you know?  
Your **location** has been shared **5398** times with Facebook, Groupon, GO Launcher EX, and 7 other apps for the past **14** days.

[Let me change my settings](#)






[Show me more before I make changes](#)

[Keep sharing my location](#)

Notification provided by AppOps.

 Your location shared with 10 apps

Number of times your **location** has been shared with each app for the past 14 days.

	Google Play services	1603
	Android System	1602
	Groupon	1602
	Weather & Clock Widget	296
	GO Launcher EX	255

[Let me change my settings](#)

[keep sharing my location](#)



# Apple and Google in mobile malware slip-up



# Anatomy of a security hole - Android Master Key

```
09-27-12 18:03 AndroidManifest.xml
09-27-12 18:03 classes.dex
09-27-12 18:03 META-INF/CERT.RSA
09-27-12 18:03 META-INF/CERT.SF
09-27-12 18:03 META-INF/MANIFEST.MF
09-27-12 18:03 res/drawable-hdpi/ic_action_search.png
09-27-12 18:03 res/drawable-hdpi/ic_launcher.png
09-27-12 18:03 res/drawable-hdpi/ic_lockscreen_handle_
09-27-12 18:03 res/drawable-hdpi/ic_menu_refresh.png
09-27-12 18:03 res/drawable-ldpi/ic_launcher.png
09-27-12 18:03 res/drawable-ldpi/ic_menu_refresh.png
09-27-12 18:03 res/drawable-mdpi/ic_action_search.png
09-27-12 18:03 res/drawable-mdpi/ic_launcher.png
09-27-12 18:03 res/drawable-mdpi/ic_lockscreen_handle_
09-27-12 18:03 res/drawable-mdpi/ic_menu_refresh.png
09-27-12 18:03 res/drawable-xhdpi/ic_action_search.png
09-27-12 18:03 res/drawable-xhdpi/ic_launcher.png
09-27-12 18:03 res/drawable-xhdpi/ic_lockscreen_handle_
09-27-12 18:03 res/drawable-xhdpi/ic_menu_refresh.png
09-27-12 18:03 res/layout/activity_demo.xml
09-27-12 18:03 res/layout/activity_main.xml
09-27-12 18:03 res/menu/activity_main.xml
09-27-12 18:03 resources.arsc
```

Original APK file

```
/Users/duck/androidmasterkey/rb-real/META-INF/
Manifest-Version: 1.0
Created-By: 1.0 (Android)
```

```
Name: res/drawable-xhdpi/ic_launcher.png
SHA1-Digest: TJE1tg63y88xLdIALKGpuLmgh0s=
```

```
Name: res/drawable-ldpi/ic_menu_refresh.png
SHA1-Digest: 2X1kJ69mGWf4m0kUHpJ6Y/v2yb4=
```

```
Name: res/drawable-mdpi/ic_action_search.png
SHA1-Digest: Y4L41d5B3tuskTn0CM7KudNT6S=
```

APK paths and filenames listed in the manifest

```
09-27-12 18:03 AndroidManifest.xml
09-27-12 18:03 classes.dex
09-27-12 18:03 META-INF/CERT.RSA
09-27-12 18:03 META-INF/CERT.SF
09-27-12 18:03 META-INF/MANIFEST.MF
09-27-12 18:03 res/drawable-hdpi/ic_ac
07-10-13 15:21 res/drawable-hdpi/ic_la
09-27-12 18:03 res/drawable-hdpi/ic_lo
09-27-12 18:03 res/drawable-hdpi/ic_me
07-10-13 15:22 res/drawable-ldpi/ic_la
09-27-12 18:03 res/drawable-ldpi/ic_me
09-27-12 18:03 res/drawable-mdpi/ic_ac
07-10-13 15:12 res/drawable-mdpi/ic_la
09-27-12 18:03 res/drawable-mdpi/ic_lo
09-27-12 18:03 res/drawable-mdpi/ic_me
09-27-12 18:03 res/drawable-xhdpi/ic_a
07-10-13 15:17 res/drawable-xhdpi/ic_l
09-27-12 18:03 res/drawable-xhdpi/ic_l
09-27-12 18:03 res/drawable-xhdpi/ic_m
09-27-12 18:03 res/layout/activity_dem
09-27-12 18:03 res/layout/activity_mai
09-27-12 18:03 res/menu/activity_main.
07-10-13 14:58 resources.arsc
```

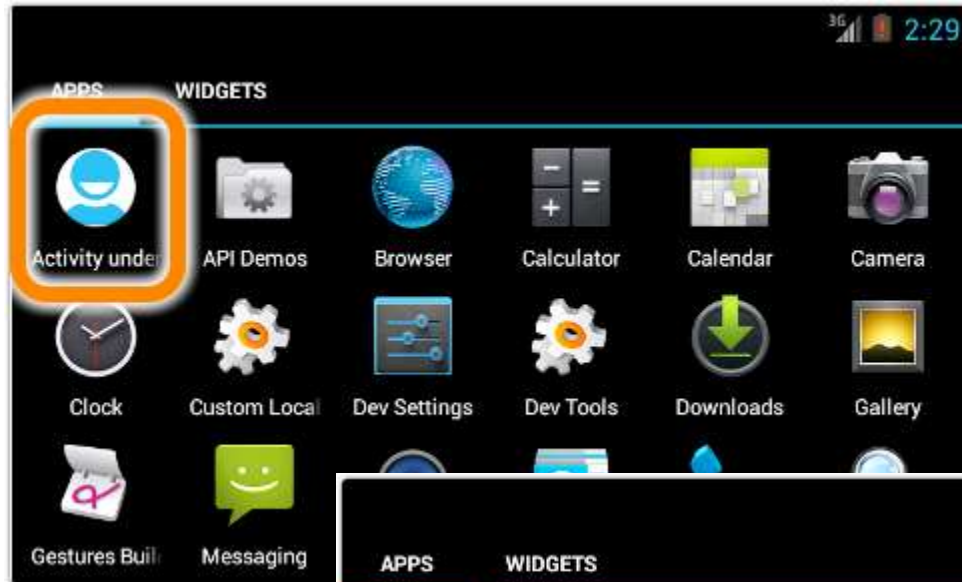
APK with changed c

```
09-27-12 18:03 AndroidManifest.xml
09-27-12 18:03 classes.dex
09-27-12 18:03 META-INF/CERT.RSA
09-27-12 18:03 META-INF/CERT.SF
09-27-12 18:03 META-INF/MANIFEST.MF
09-27-12 18:03 res/drawable-hdpi/ic_action_search.png
09-27-12 18:03 res/drawable-hdpi/ic_launcher.png
09-27-12 18:03 res/drawable-hdpi/ic_lockscreen_handle_pressed.png
09-27-12 18:03 res/drawable-hdpi/ic_menu_refresh.png
09-27-12 18:03 res/drawable-ldpi/ic_launcher.png
09-27-12 18:03 res/drawable-ldpi/ic_menu_refresh.png
09-27-12 18:03 res/drawable-mdpi/ic_action_search.png
09-27-12 18:03 res/drawable-mdpi/ic_launcher.png
09-27-12 18:03 res/drawable-mdpi/ic_lockscreen_handle_pressed.png
09-27-12 18:03 res/drawable-mdpi/ic_menu_refresh.png
09-27-12 18:03 res/drawable-xhdpi/ic_action_search.png
09-27-12 18:03 res/drawable-xhdpi/ic_launcher.png
09-27-12 18:03 res/drawable-xhdpi/ic_lockscreen_handle_pressed.png
09-27-12 18:03 res/drawable-xhdpi/ic_menu_refresh.png
09-27-12 18:03 res/layout/activity_demo.xml
09-27-12 18:03 res/layout/activity_main.xml
09-27-12 18:03 res/menu/activity_main.xml
09-27-12 18:03 resources.arsc
09-27-12 18:03 resources.arsc
09-27-12 18:03 res/drawable-hdpi/ic_launcher.png
09-27-12 18:03 res/drawable-ldpi/ic_launcher.png
09-27-12 18:03 res/drawable-mdpi/ic_launcher.png
09-27-12 18:03 res/drawable-xhdpi/ic_launcher.png
```

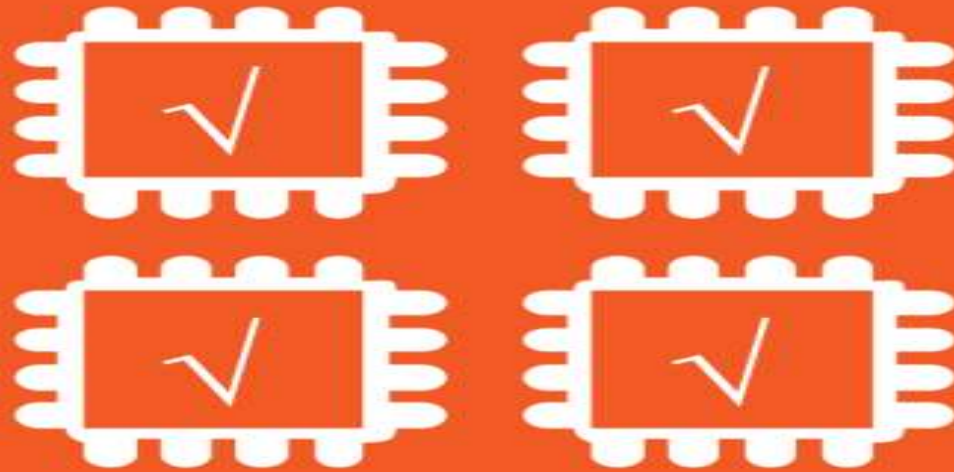
Hacked APK with changed files duplicated in archive



# Anatomy of a security hole - Android Master Key



# Quadrooter – the biggest bugs ever found





# Apple iOS – zero-day attack seen in the wild

## 1. WebKit bug:

visiting a maliciously crafted website may lead to arbitrary code execution.

## 2. Kernel bug:

an application may be able to disclose kernel memory.

## 3. Kernel bug:

an application may be able to execute arbitrary code with kernel privileges.



# FBI cracks \*that\* iPhone



IN THE MATTER OF THE SEARCH  
OF AN APPLE IPHONE SEIZED  
DURING THE EXECUTION OF A  
SEARCH WARRANT ON A BLACK  
LEXUS IS300, CALIFORNIA  
LICENSE PLATE #5KGD203

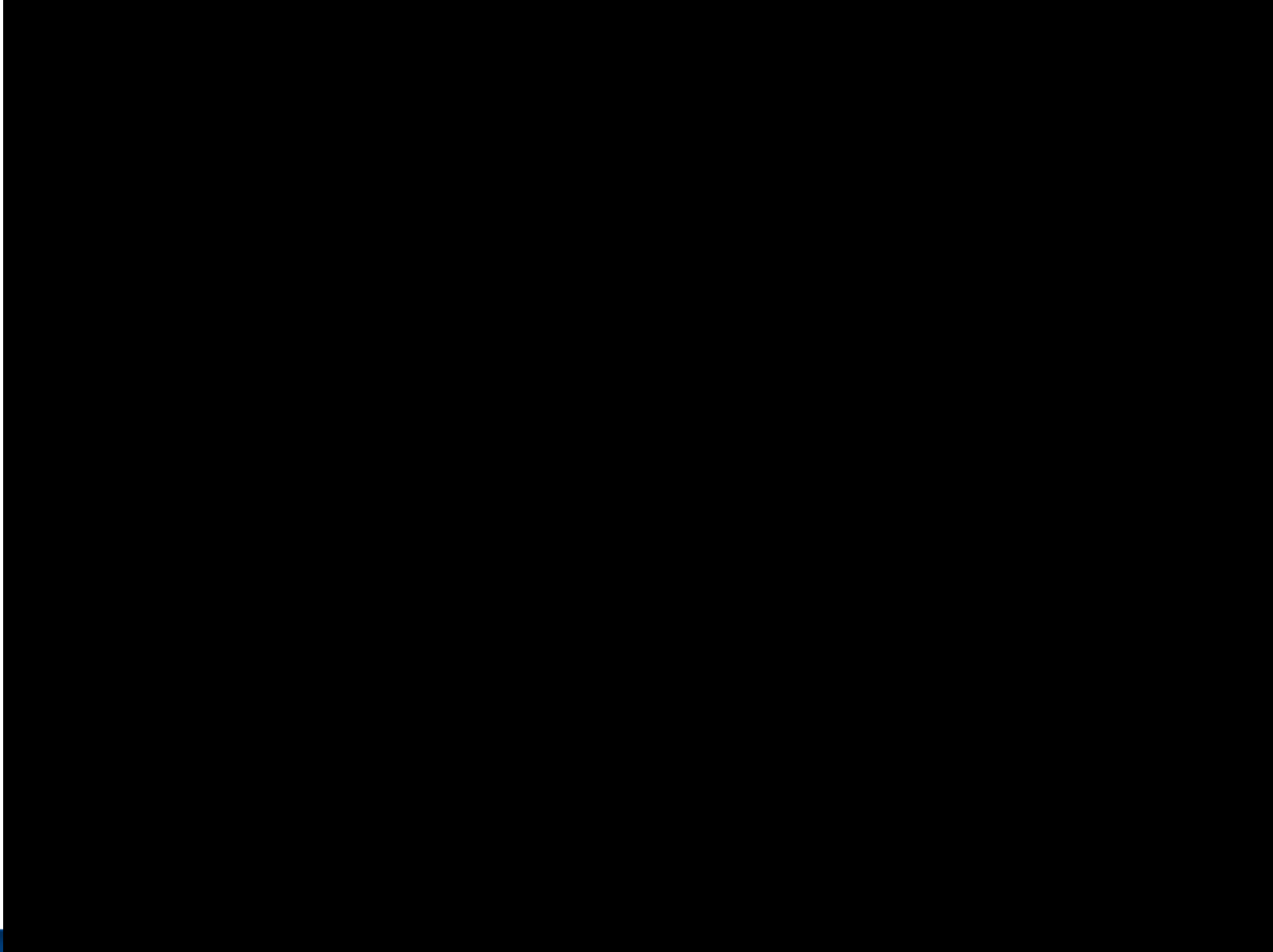
ED No. CM 16-10 (SP)

GOVERNMENT'S STATUS REPORT

The government has now successfully accessed the data stored on Farook's iPhone and therefore no longer requires the assistance from Apple Inc. mandated by Court's Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016.

Accordingly, the government hereby requests that the Order Compelling Apple Inc. to Assist Agents in Search dated February 16, 2016 be vacated.

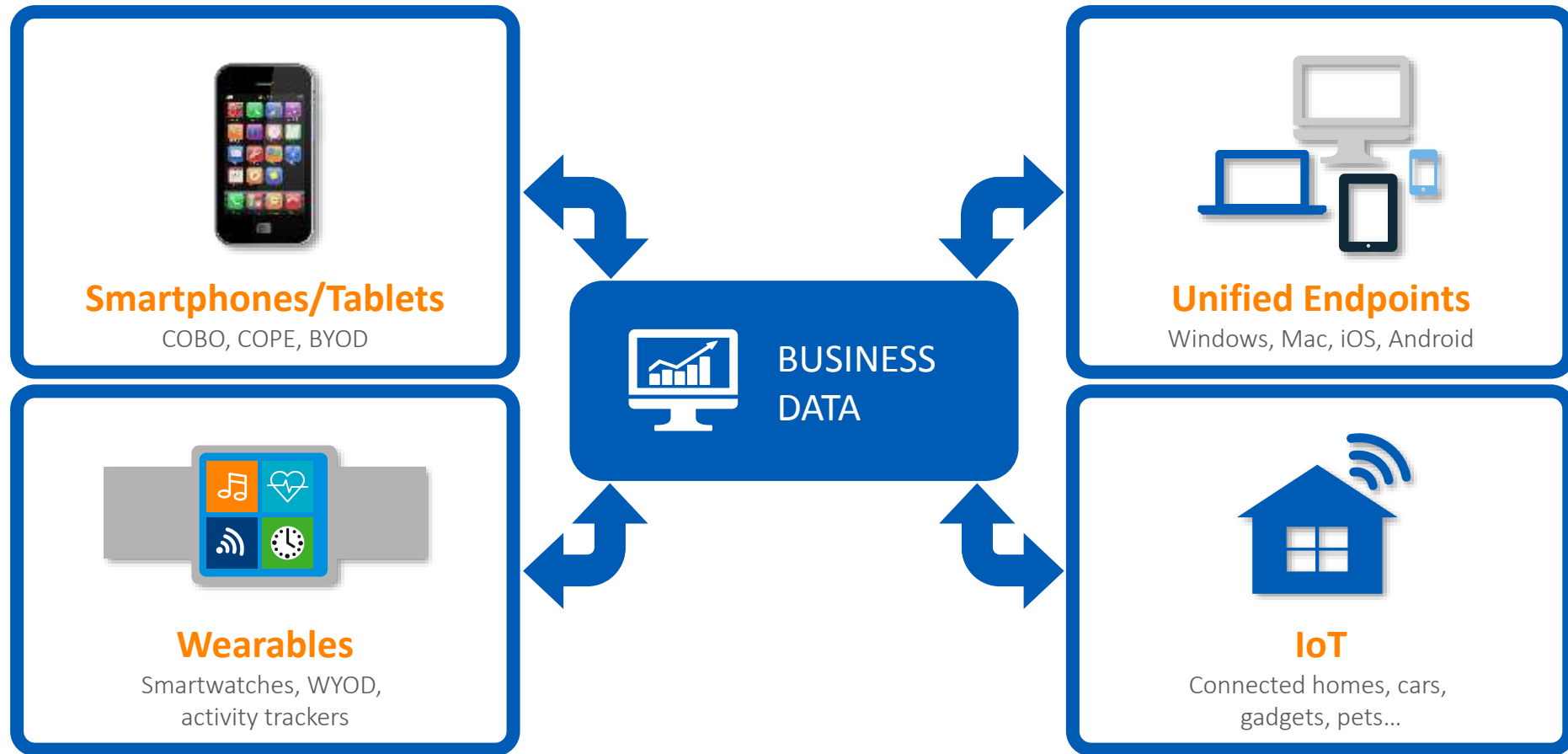
FBI or no FBI – how you can crack an iPhone for less than \$100



# Mobile Management

**SOPHOS**

# Mobility Management Tomorrow



# Why Is Managing Mobile Devices Important?

**Enabling** use of mobile devices lets users be **productive** – but comes at a price:

Users want to access **everything**,  
from **anywhere**, all the time

Users find a way to access business resources  
on **unsecured** devices

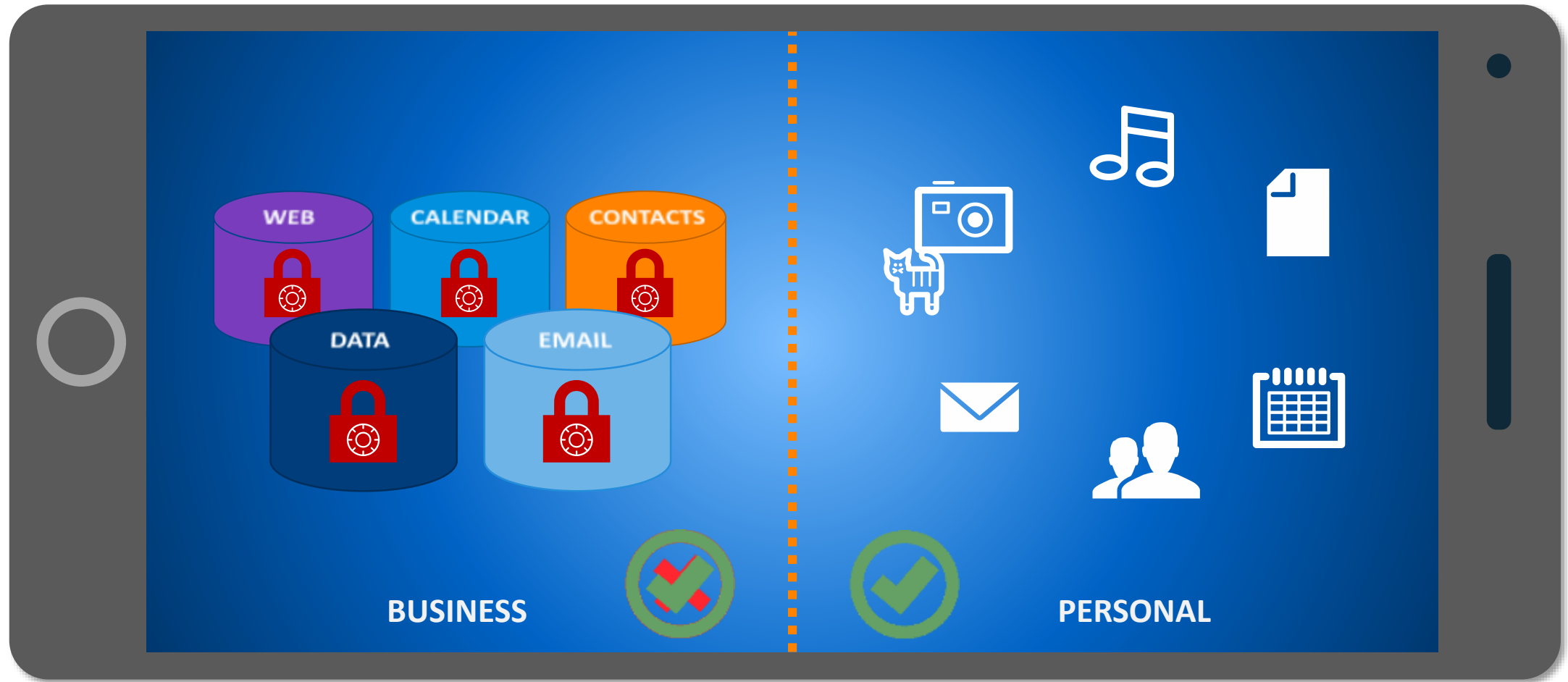
Not managing mobile devices means flying blind,  
with **zero visibility**

**Manage** your mobile devices with  
Mobile Control and limit the risks

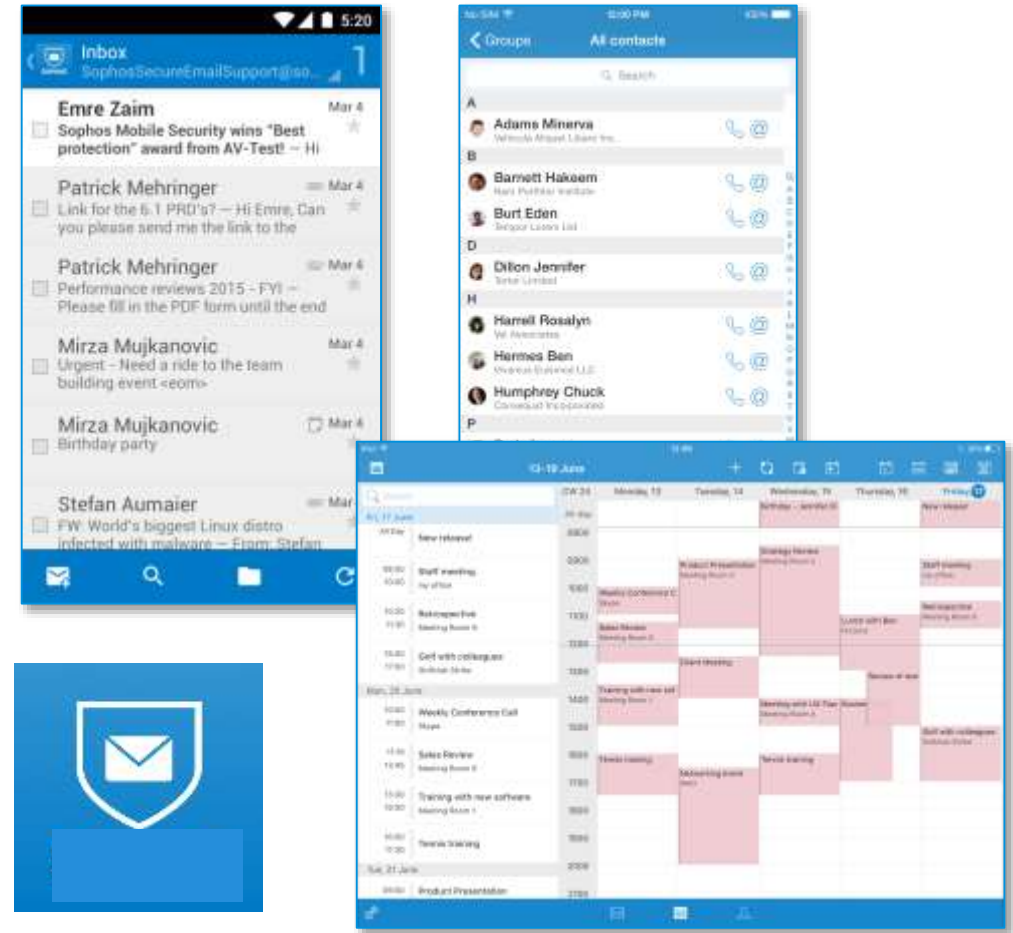
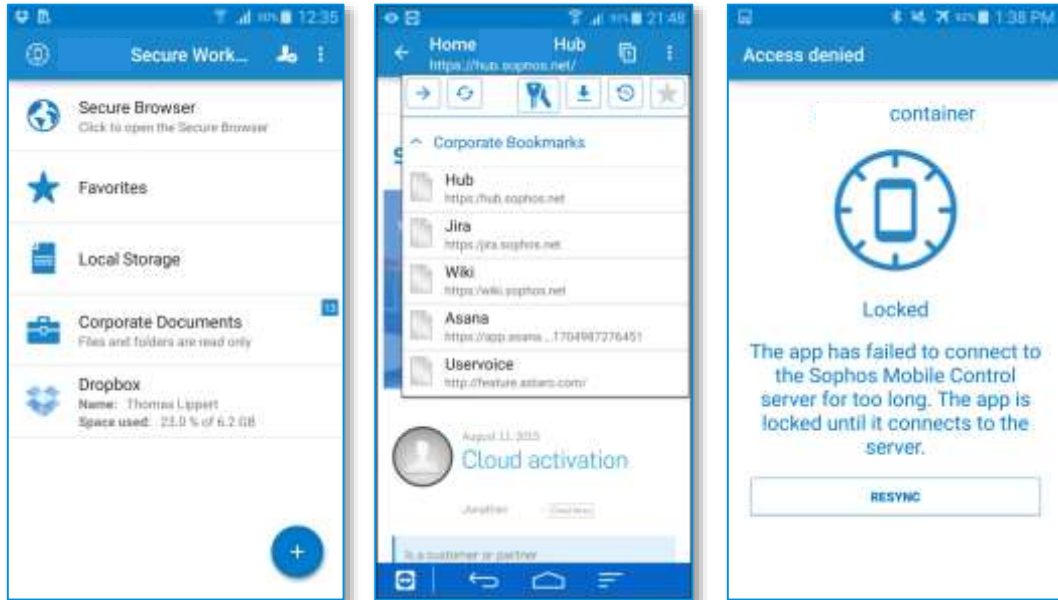




# Containers – Separate Business and Personal Data



# Container Apps

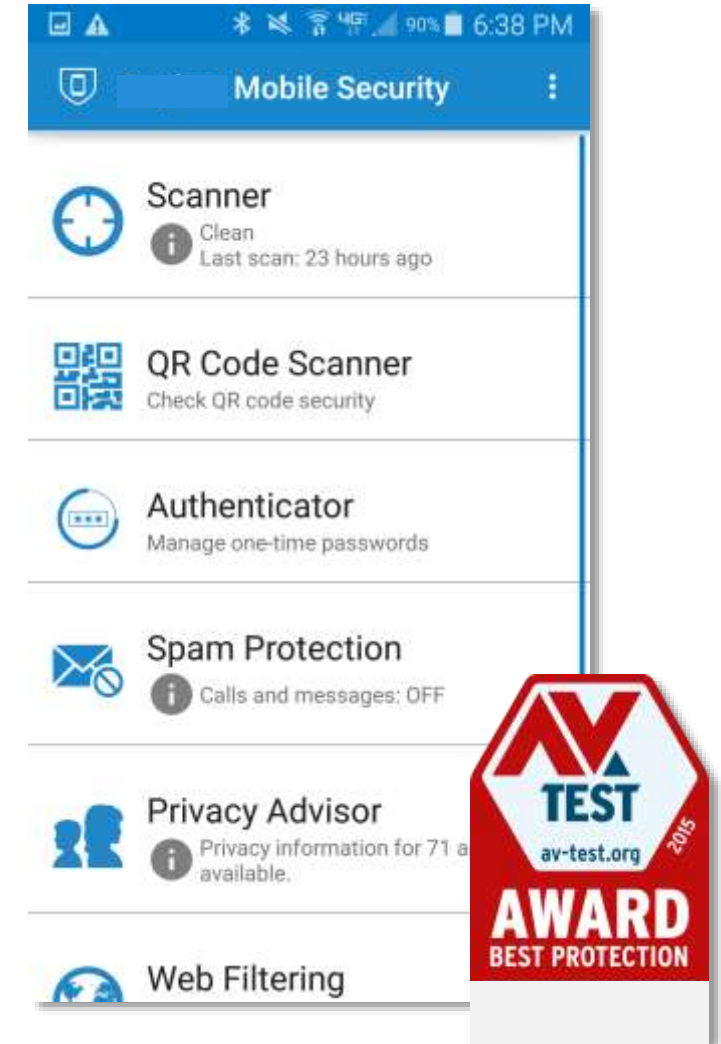


# Mobile Security

**SOPHOS**

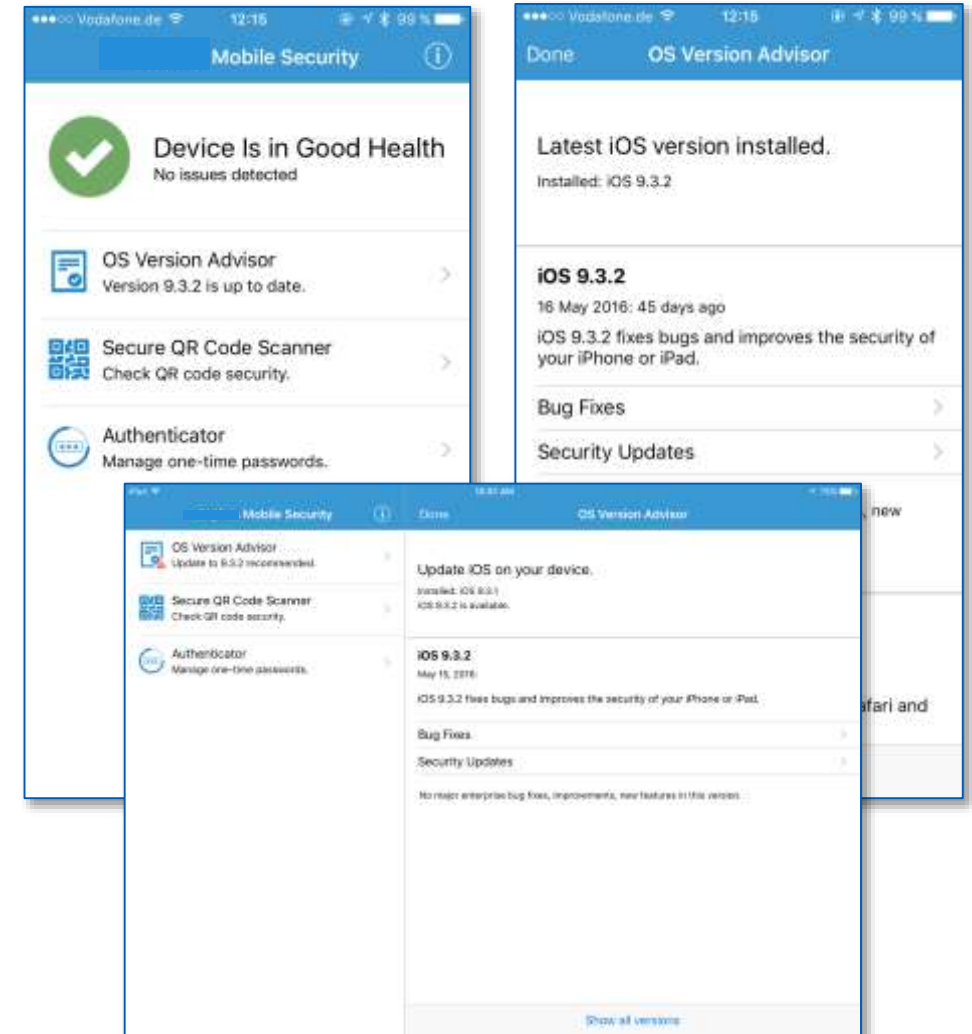
# Mobile Security for Android

- Award-winning mobile AV and Malware protection
- Web Filtering
- Spam Protection
- Additional security tools and advisors
  - Privacy Advisor
  - Authenticator
  - Secure QR Code Scanner
- Centrally Managed



# Mobile Security for iOS

- AV on iOS is inefficient
- Vulnerabilities are best fought by staying up-to-date
- Mobile Security for iOS version 1.0:
  - OS Version Advisor
  - Secure QR Code Scanner
  - Authenticator
- Not managed



# Mobile Security Challenges





# Mobile Security Challenges

- **An unsecured device means unsecured data**
  - You can insure your devices – but what is your data worth?
- **EMM helps enforce controls such as password, lock, etc.**
  - If you're not sure, you're not secure
- **Protect Android devices with anti-malware protection**
  - Users can remove protection, so needs to be enforced
- **Malicious websites can also target mobile users**
  - Apply web protection to keep web threats at bay



**SOPHOS**  
Security made simple.