

THEODORA TITONIS

VERACODE

Vice President Mobile

Public Safety Communications Research
June 4, 2014



MOBILE SECURITY

Increasing Threat



47%

Nearly half of companies that permit BYOD experienced a **data or security breach** as a result of an employee-owned device accessing the corporate network.¹



64%

Companies with **no BYOD policy**.³



34%

Companies with **no app security program**.⁴



66%

Enterprises have had **undisclosed** data breaches.²



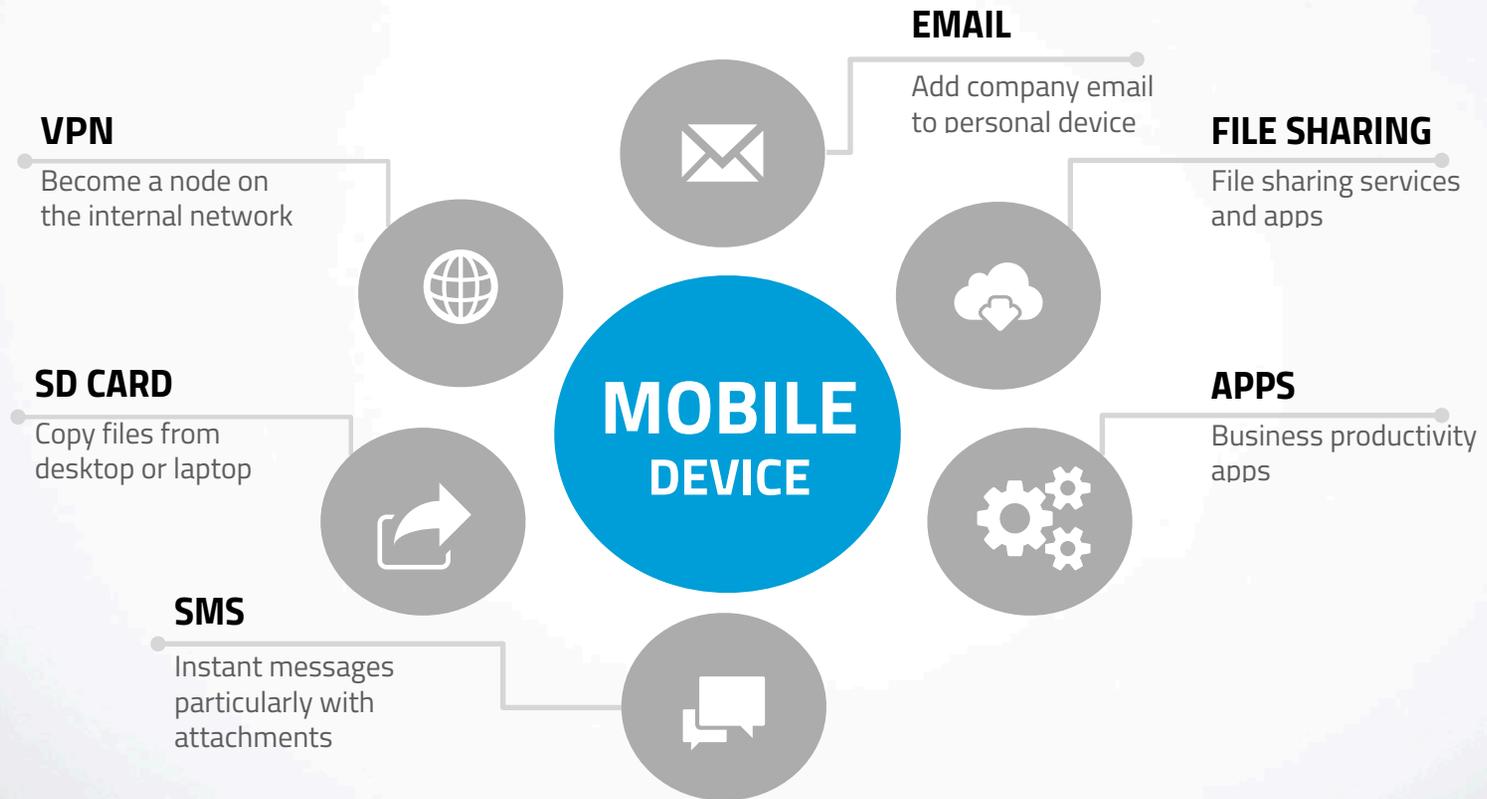
614%

Mobile threat increase over the past year. A dramatic rise from 155% in the previous year.⁵

- 1 August 2012 Decisive Analytics, LLC, Mobile Consumerization Trends & Perceptions
- 2 November 2013 Opinion Matters, Threat Track Security
- 3 June 2013 Cisco BT, Impact of BYOD on Enterprise Networks
- 4 December 2012 SANS, Survey on Application Security Programs and Practices
- 5 June 2013 Juniper, Mobile Threat Report

MOBILE SECURITY

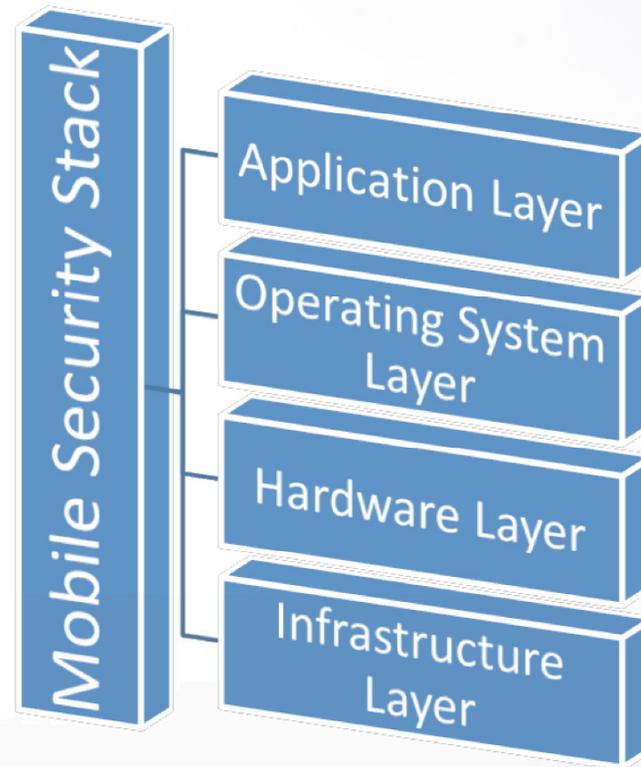
Sensitive Data on Mobile Device



MOBILE SECURITY STACK

Description of Layers

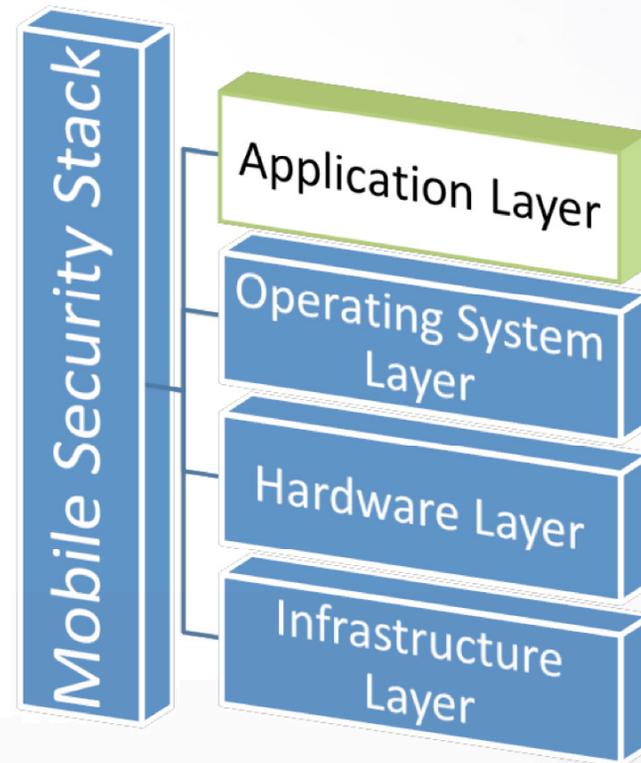
- ✓ Well-defined layers
- ✓ An abstraction based model
- ✓ Allows for focus on specific area of concern/expertise
- ✓ Results in a comprehensive approach



MOBILE SECURITY STACK

Application Layer

- ✓ More app downloads than stars in our galaxy by 2017
- ✓ Software that the end-user directly interfaces with
- ✓ Utilizes the API's provided by the operating system (OS)
- ✓ Interfaces with the cloud or the device through the OS



Applications are the engine for innovation and *the* primary target for cyber-attacks

Application Layer

More than 50% of all attacks now target the application layer* — yet fewer than 10% of enterprises test all of their business-critical applications**.

Network

Web/App Server

Database

Operating System

* Verizon DBIR

** SANS

MOBILE APP SECURITY

Securing Apps that are Produced and Consumed

APP PRODUCER

Mobile SDLC:

-  **Volume:** 10-100s of apps
-  **Speed:** New apps every quarter
-  **Choice:** Developer driven

APP CONSUMER

BYOD (or BYOA):

-  **Volume:** Thousands of apps
-  **Speed:** New apps every day
-  **Choice:** Employee Driven



ENTERPRISE VIEW OF MOBILE APPS

Access Sensitive Corporate Data

Internally Developed Apps

This class of app leaves the enterprise most exposed to risk. Financial services, healthcare, highly regulated industries.



Business Apps (Supply Chain)

This class of app accesses "customer sensitive" data and therefore is a risk for enterprises.



Consumer Apps

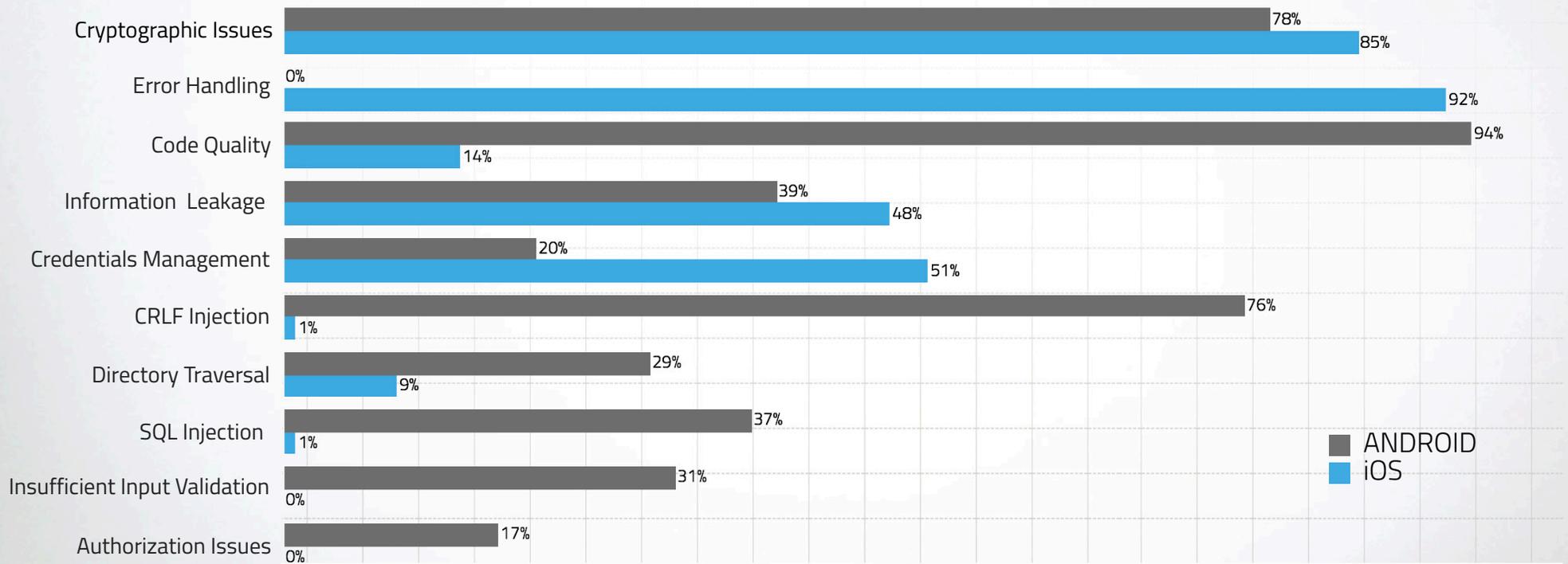
This class of app resides on employee devices alongside internally developed and business apps.



MOBILE APPS

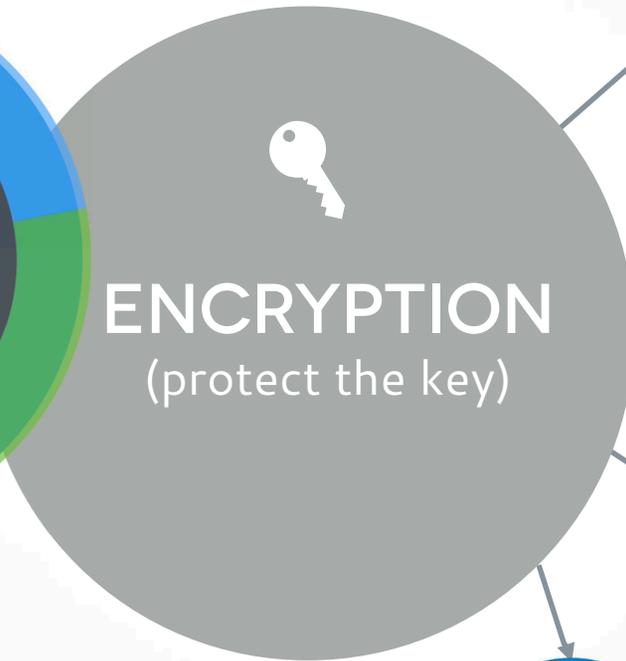
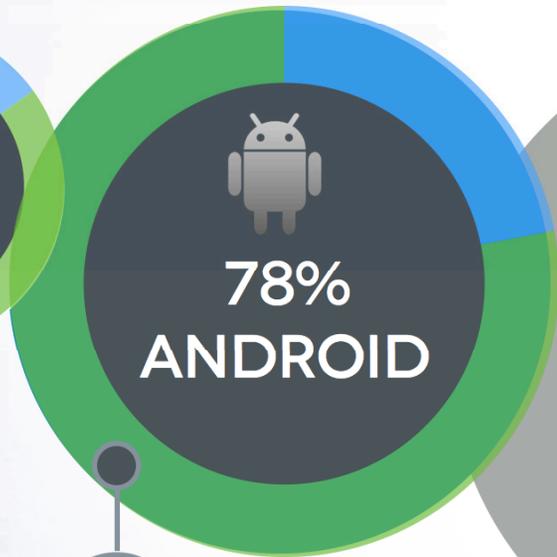
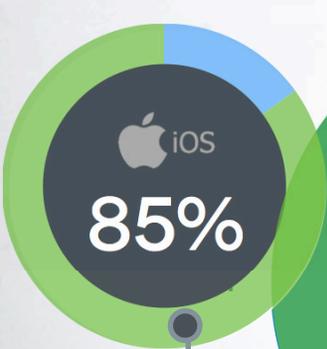
Vulnerabilities

Top Vulnerabilities



MOBILE APPS

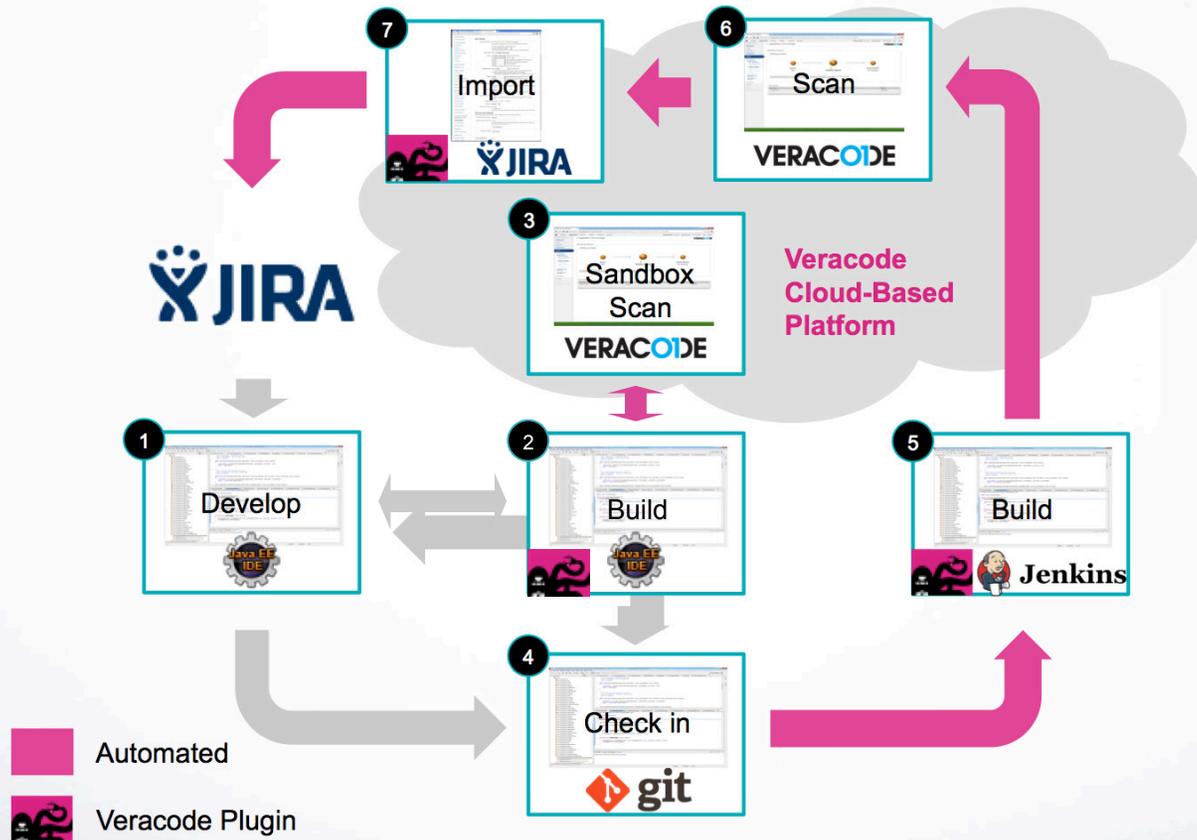
Cryptographic Issues



CRYPTOGRAPHIC ISSUES

POLICIES FOR APPS PRODUCED

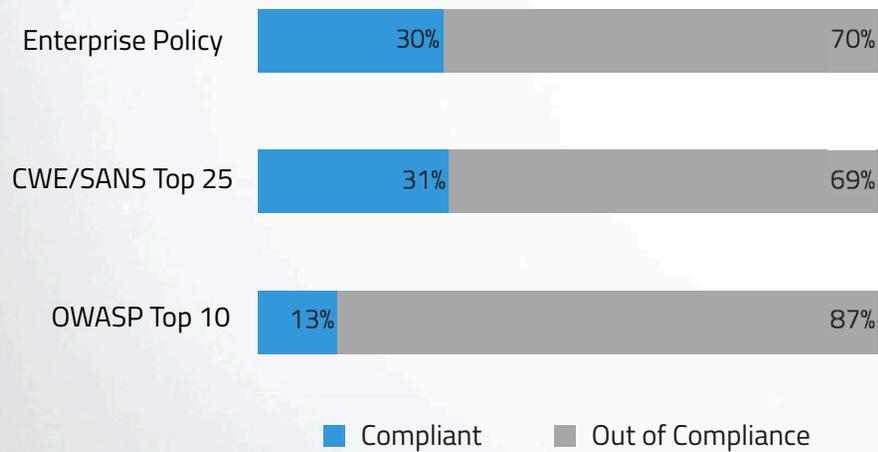
Security as Part of the Software Development Lifecycle



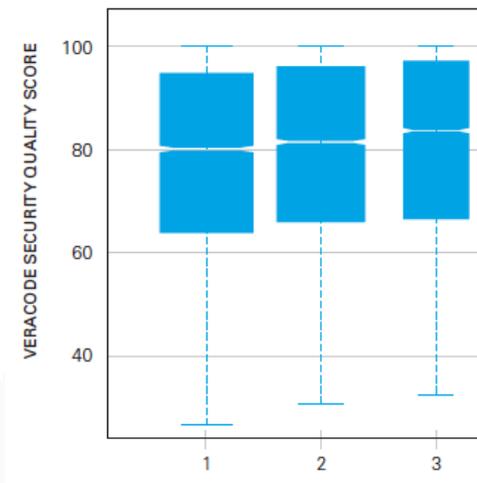
POLICIES FOR APPS PRODUCED

SECURITY AS PART OF SOFTWARE DEVELOPMENT LIFECYCLE

Compliance with Policies
Upon First Submission

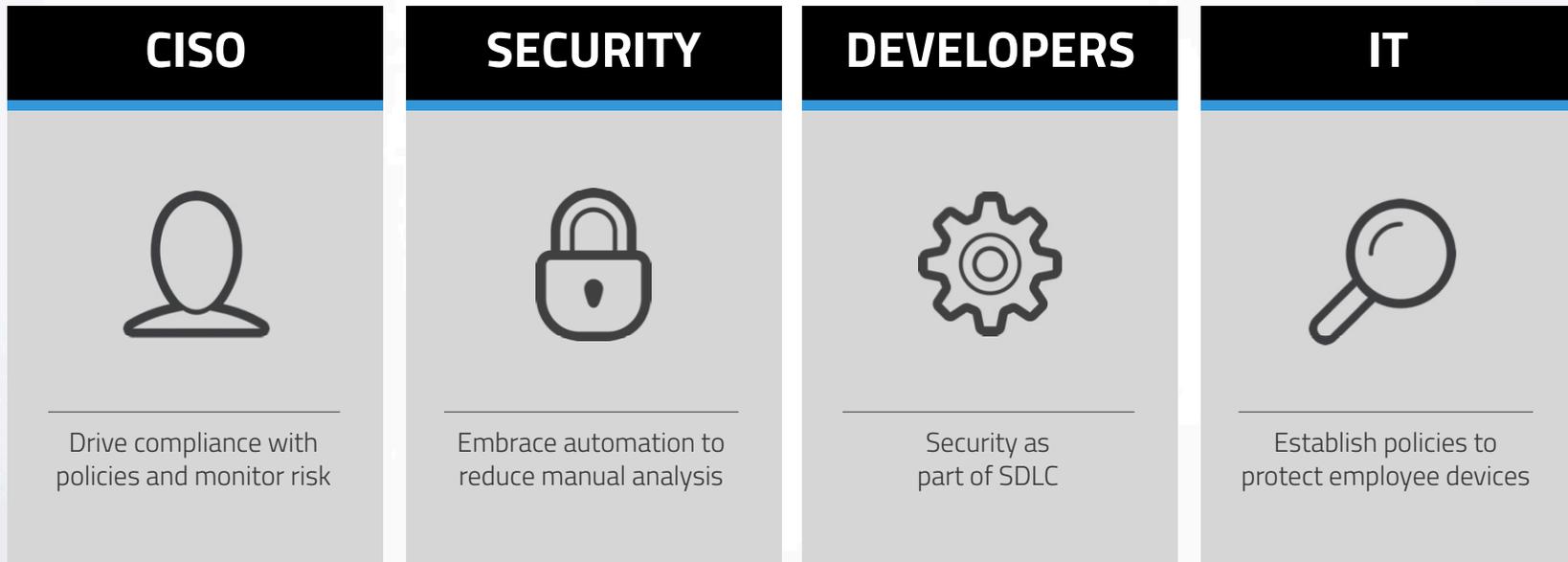


Significant Improvement
in First Three Builds



CUSTOM MOBILE APP SECURITY POLICIES

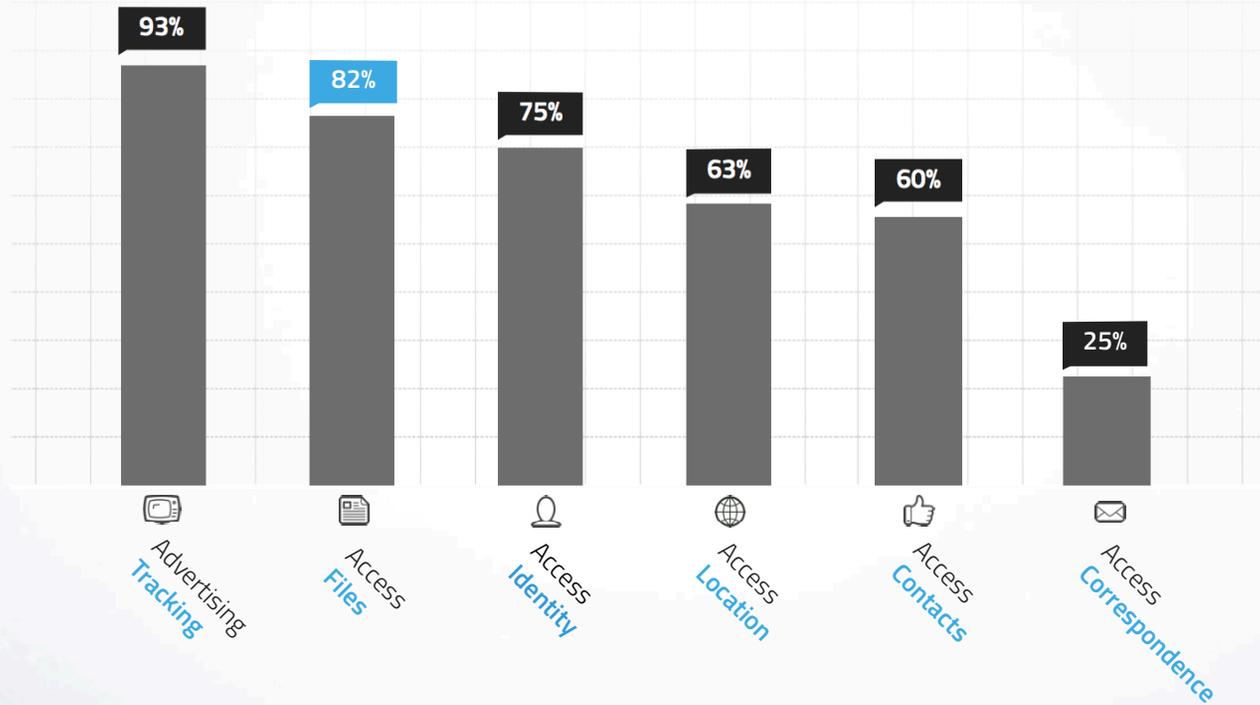
Collaborative Effort Between Business, IT, and Security



MOBILE APPS

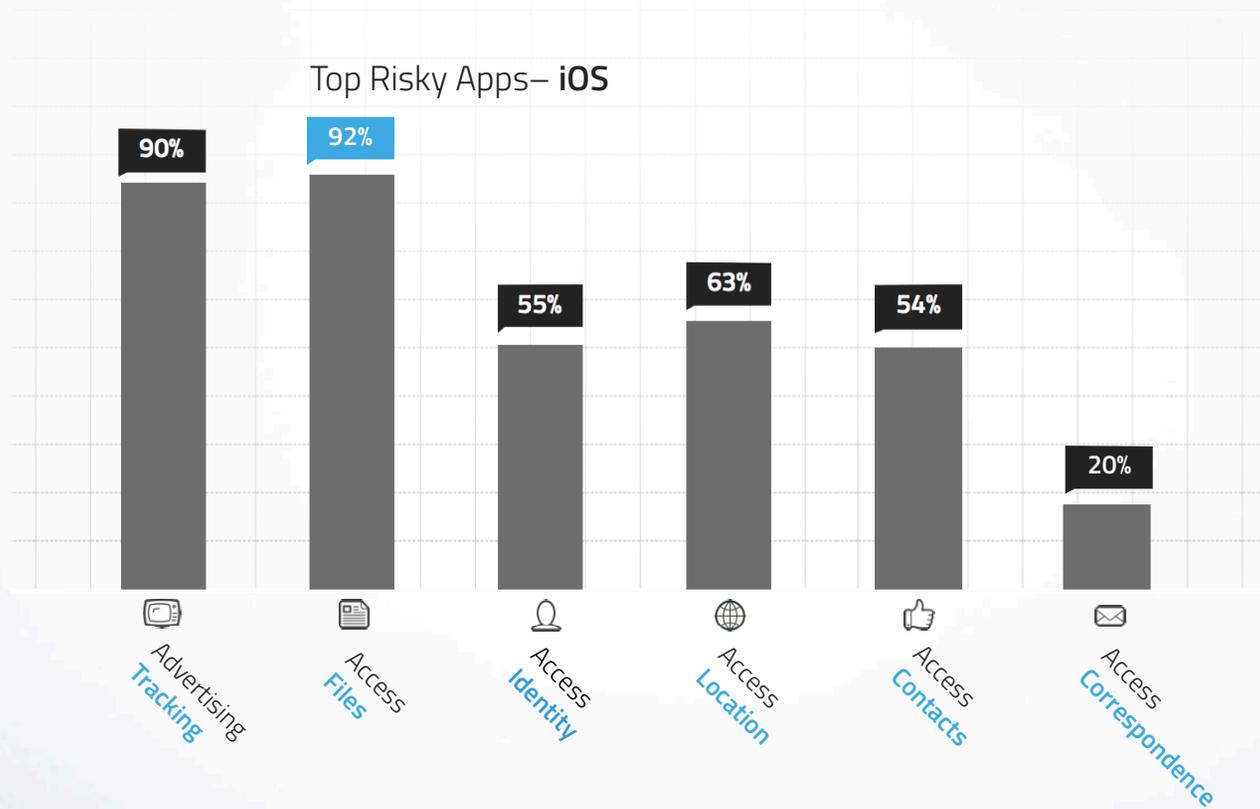
Android and iOS Risky Apps

Top Risky Apps– **Android**



MOBILE APPS

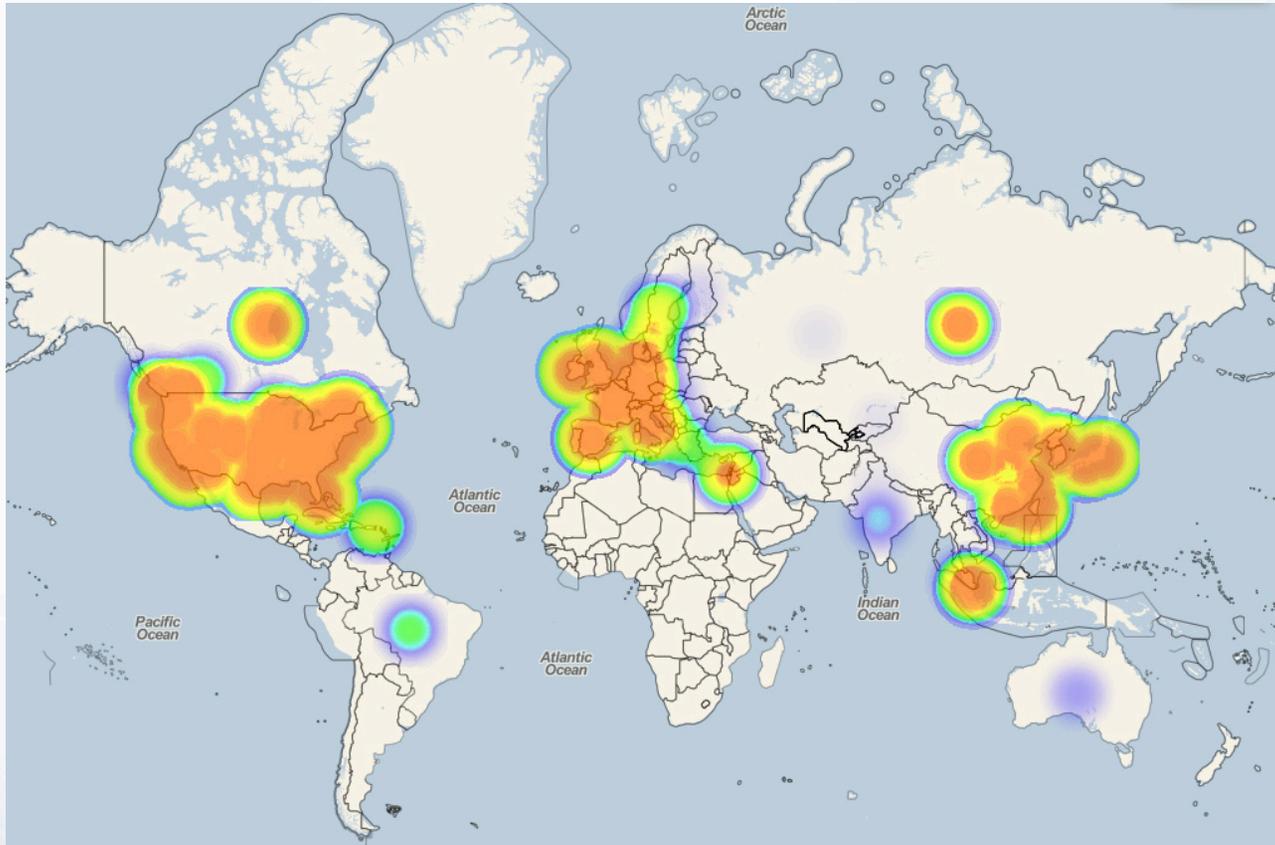
Android and iOS Risky Apps



MOBILE APPS

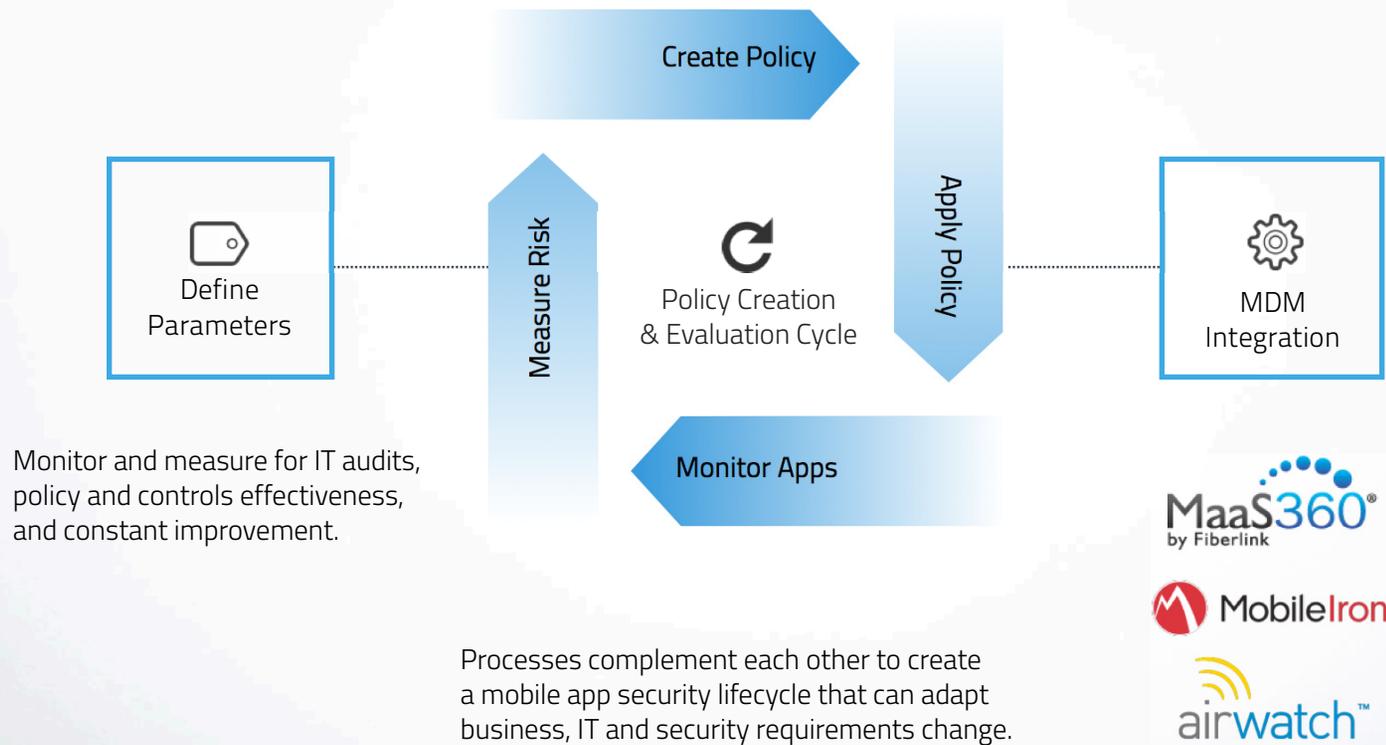
Android and iOS Risky Apps

Top Apps – **Android**



CUSTOM MOBILE APP SECURITY POLICIES

Strategic, Comprehensive, and Policy-Driven Approach



DATA LOSS PREVENTION

Securing Sensitive Data

Sensitive unencrypted network data

- ✓ Direct HTTP Access
- ✓ Direct Socket Access

Sensitive unencrypted SQLite data

APPLY POLICY TO PROHIBIT APPS

- ✓ Uses SQLITE

Sensitive unencrypted filesystem data

- ✓ Examine Filesystem
- ✓ Read Files

DATA LOSS PREVENTION

Sensitive Data by Organization or Role

iOS

92%

20%

54%

55%

63%

30%

Android

82%

25%

60%

75%

63%

70%



FILES

CORRESPONDENCE

CONTACTS

IDENTITY

LOCATION

DEVICE

- Read Files
- Access Cloud Resources
- USB Usage
- Examine File System
- Retrieve Browser History
- Access Cookies
- Access to Bookmarks

- Read SMS Messages
- Send, Receive, Prepare SMS
- Consume SMS Messages
- Access Call Log
- Record Phone Calls
- Monitor Phone Calls

- Read Contacts
- Write Contacts
- Edit Contacts
- Track Address Book
- Bulk Access Contacts
- Access Facebook Audience

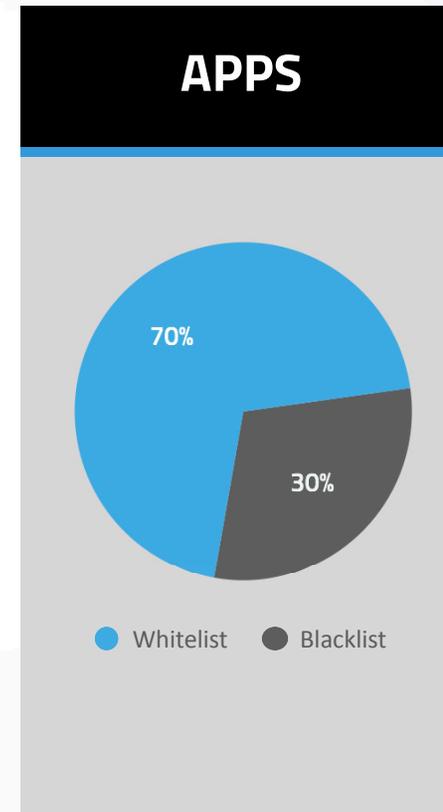
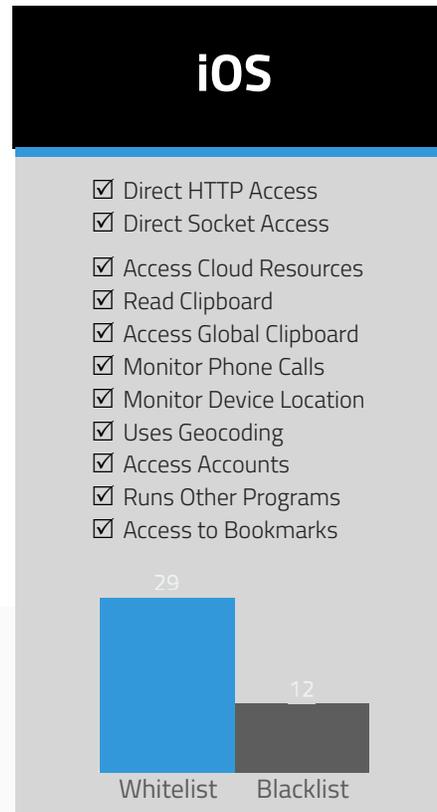
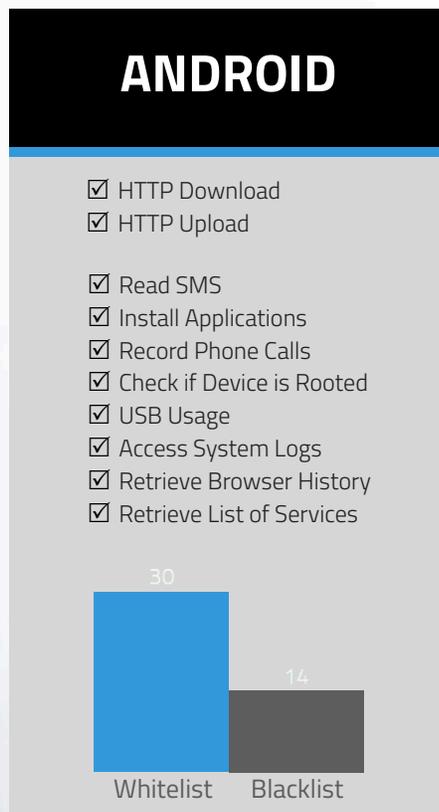
- Examine Android Account
- Access Unique Device ID
- Retrieve SIM Card Info
- Access Social Networks
- Access Facebook
- Access Twitter
- Access Accounts

- Monitor Location
- Uses Geocoding

- Root Device
- Listen for Key Presses
- Monitor Phone Activity
- Monitor Camera Interface
- Capable of Recording Audio
- Access System Logs
- Retrieve List of Running Apps
- Access to Shared Library
- Access to Default Preferences

CUSTOM MOBILE APP SECURITY POLICIES

Access to Sensitive Data with use of Unencrypted Network Data



CUSTOM MOBILE APP SECURITY POLICIES

Access to Sensitive Data with use of Unencrypted Network Data

Apps that **Check if a Device is Rooted**

Code exists to determine if the device has been rooted/jailbroken and running in superuser/admin mode.



Afarria
Android



Netflix
Android



Pandora
Android



Twitter
Android



Yelp
Android

Apps that **Access System Logs**

Has code necessary to read log files such as system events, application events and other output.



Divide
Android



Instagram
Android



iPass
Android



LinkedIn
Android



Receiver
Android



SAP BI
Android



Skype
Android



TripAdvisor
Android



Yelp
Android

CUSTOM MOBILE APP SECURITY POLICIES

Access to Sensitive Data with use of Unencrypted Network Data

Apps that **Bulk Access Contacts**

Contains code capable of reading and/or copying all data from your address book. May also mass import from a vcard source.



Instagram
iOS



Find My Friends
iOS



Google Search
iOS



Pandora
iOS



SAP Business Objects Mobile
iOS



Skype
iOS



Symantec Mobile Encryption
iOS



Twitter
iOS



Facebook
iOS

Apps that **Runs Other Programs**

Contains code that can execute other programs which may also return data back to it.



Google Search
iOS



Netflix
iOS



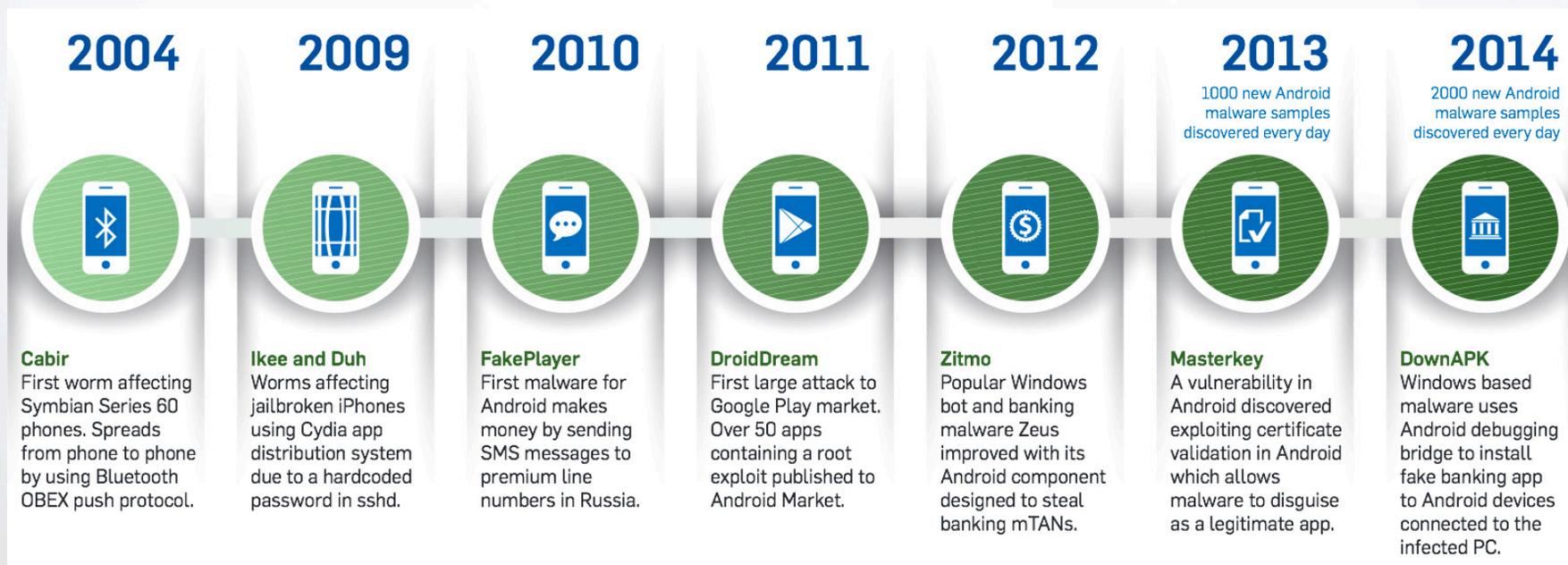
Pandora
iOS



Symantec Mobile Encryption
iOS

MALWARE

Decade of Mobile Malware*



*Sophos Mobile Threat Report, Mobile World Congress, 2014

MALWARE

Android Malware Samp



SALTED HASH-TOP SECURITY NEWS
By Steve Ragan

About | Fundamental security insight to help you minimize risk and protect your organization

NEWS

Symantec develops new business strategy, says AV is dead

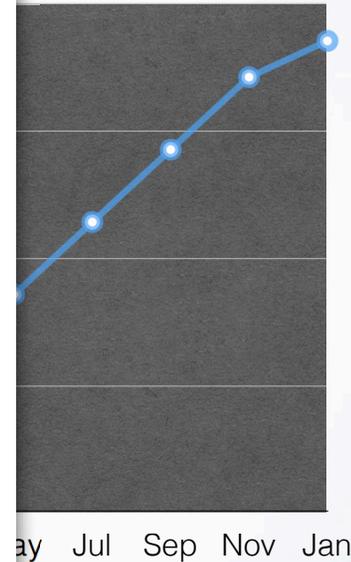
Symantec says that AntiVirus is dead, citing it as one of the reasons they're shifting focus and mapping out a new plan of attack when it comes to dealing with threats

CSO | May 5, 2014 3:27 PM

Symantec says that Anti-Virus is dead, citing it as one of the reasons they're shifting focus and mapping out a new plan of attack when it comes to dealing with threats.

On Sunday, [in an interview with the Wall Street Journal](#), Symantec's VP of Information Security, Brian Dye, said that Anti-Virus was dead, adding that the company didn't view it as a moneymaker anyway. Dye's comments were part of a story on Symantec's new direction, which includes harm minimization as well as incident response.

According to the Journal, Symantec said that they expect to start selling threat intelligence and offering incident response to recently compromised firms within six months.



*Sophos Mobile Threat Report, Mobile World Congress, 2014

CUSTOM MOBILE APP SECURITY POLICIES

Collaborative Effort Between Business, IT, and Security

