



# GPDR & Mobility : Securing Mobile

Tom Davison, EMEA SE Mgr | Friday 3<sup>rd</sup> February 2017

The world has changed.



The data center is a cloud.

The corporate network is Starbucks WiFi.



A grayscale photograph of a person's hands holding a smartphone. The person is wearing a dark jacket. In the foreground, a Herschel bag is visible with two leather watch straps resting on it. The text "Phones, tablets, and wearables have replaced managed laptops." is overlaid in white on the image.

Phones, tablets, and wearables have replaced managed laptops.



The hottest new apps are built in  
someone's garage.

A close-up, grayscale photograph of a person's hand holding a smartphone. The hand is positioned in the center-left of the frame, with the fingers gripping the device. The background is dark and out of focus. Overlaid on the image is white text in a clean, sans-serif font.

The new world of choice puts  
your data in the hands of users,  
and out of your control.



# 51%

Time on mobile, vs  
42% on PC

# 90%

Time in apps,  
not the browser.

OS and form factors are  
converging

**KPCB** | KLEINER  
PERKINS  
CAUFIELD  
BYERS

 **FLURRY**

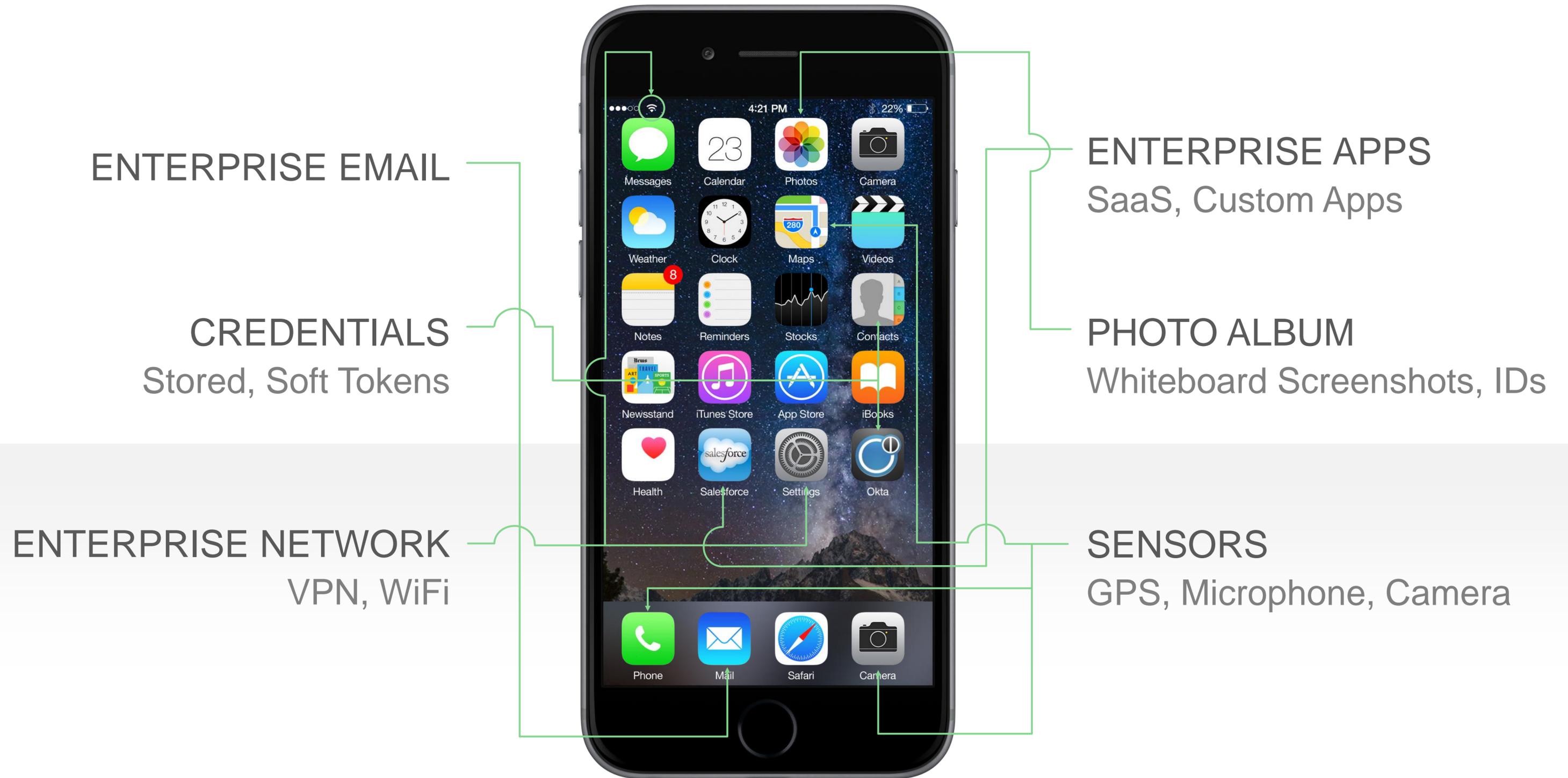
   
Windows 10



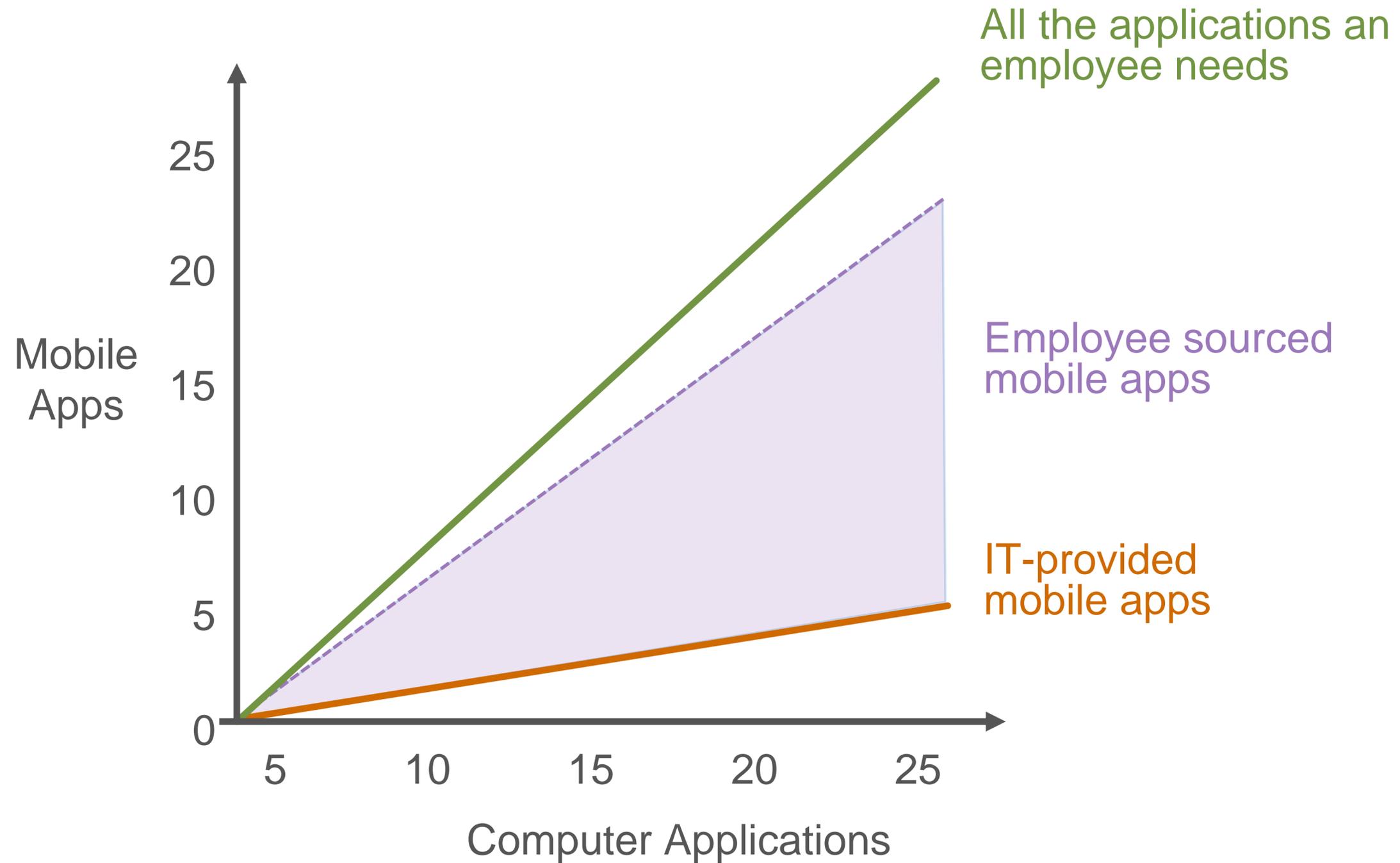
Risk =

$$\frac{\text{threats} \times \text{vulnerabilities}}{\text{controls}} \times \text{asset value}$$

# Consider the data on you mobile device



# APP SOURCING



# SALES MASHUP

### ACME Manufacturing

Bob Smith  
COO

125 Main St  
Freemont, CA 94536

**Mobile:** [+1\(408\) 555-1534](tel:+14085551534)  
**Work:** [+1\(408\) 555-8461](tel:+14085558461)



<b>Opportunity</b>	<b>Forecast</b>	<b>Mon Oct-14, 10:32am</b>	<a href="#">New</a>
120k users	<b>80%</b>	Bob to assign Director (Kevin?) to project and provide requirements.	<a href="#">Edit</a>
14k apps	<b>60%</b>	<b>Thu Oct-10 9:12am</b>	<a href="#">Edit</a>
		Bob said he is unlikely to get budget for this project, but will find out more in planning...	

<b>History</b>	<b>SA</b>	<b>Details</b>
8.2k users	30-Jun-15	BYOD project "Choice" led by Bob. Rollout staged...
1,600 apps	31-Dec-14	Infrastructure update to enable DR and Business...
2,000 users	30-Jun-14	Initial purchase for Networking group for Project...
100 users	30-Jun-14	Proof-of-concept purchase for Project Choice (BY...

### Customer Care

Failed Login ⚠ **Mon Oct-14, 8:15am** Provided work-around for login issue...

Appliance F... ✖ **Tue Oct-1, 3:22pm** Replaced faulty NIC under warranty usi...

  
Customer

  
Opportunity

  
Pipeline

  
Activity

  
Reports

# SALES MASHUP

salesforce.com

LinkedIn

Contacts

salesforce.com

SAP

License tracking db

Bugzilla

### ACME Manufacturing

Bob Smith  
COO

125 Main St  
Freemont, CA 94536

**Mobile:** +1(408) 555-1534  
**Work:** +1(408) 555-8461

Opportunity	Forecast	Activity
120k users	80%	<b>Mon Oct-14, 10:32am</b> Bob to assign Director (Kevin?) to project and provide requirements.
14k apps	60%	<b>Thu Oct-10 9:12am</b> Bob said he is unlikely to get budget for this project, but will find out more in planning...

History	SA	Details
8.2k users	30-Jun-15	BYOD project "Choice" led by Bob. Rollout staged...
1,600 apps	31-Dec-14	Infrastructure update to enable DR and Business...
2,000 users	30-Jun-14	Initial purchase for Networking group for Project...
100 users	30-Jun-14	Proof-of-concept purchase for Project Choice (BY...

### Customer Care

Failed Login	⚠	<b>Mon Oct-14, 8:15am</b> Provided work-around for login issue...
Appliance F...	✖	<b>Tue Oct-1, 3:22pm</b> Replaced faulty NIC under warranty usi...

Customer Opportunity Pipeline Activity Reports

Google Maps

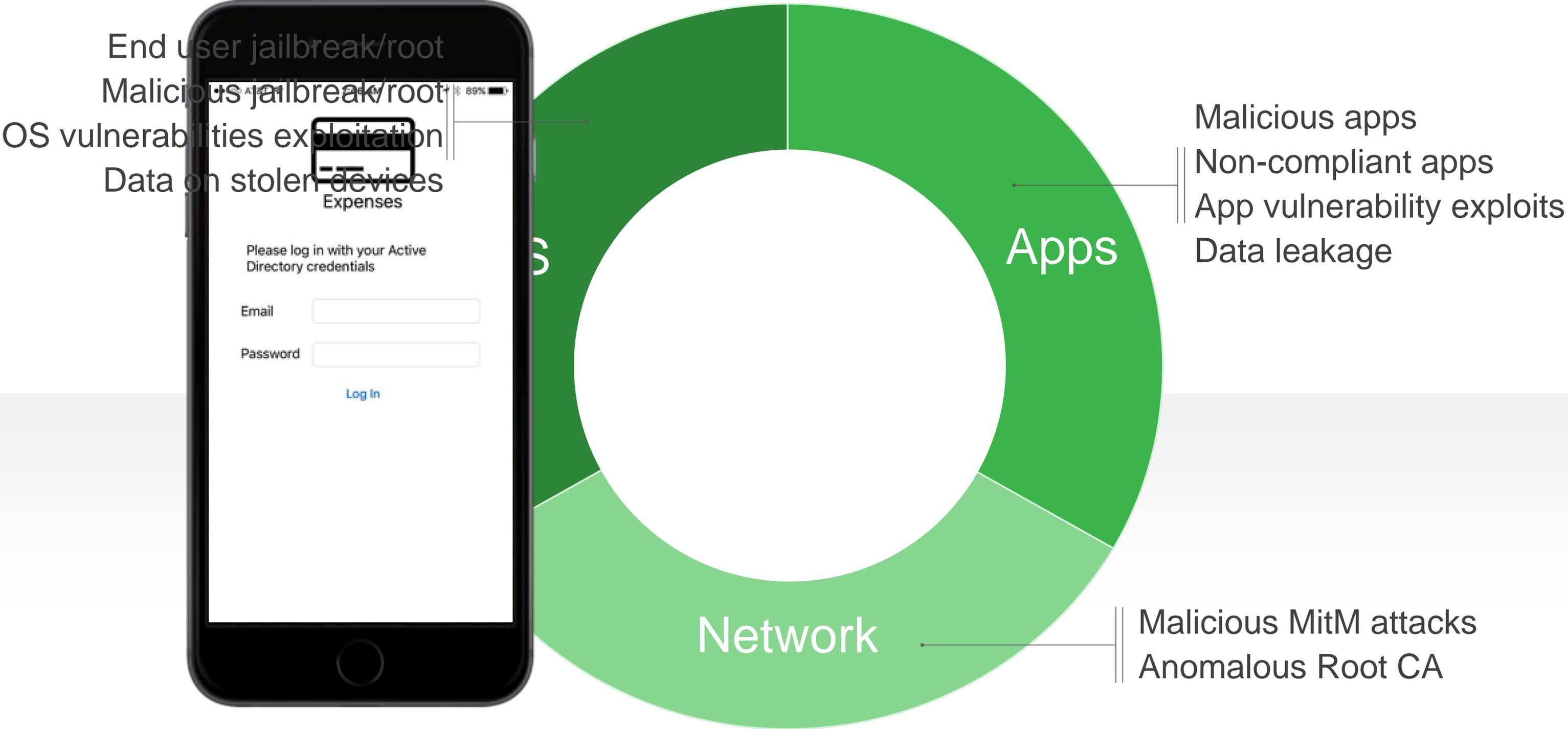
salesforce.com

— SaaS API

— Legacy System API

$$\frac{\text{threats} \times \text{vulnerabilities}}{\text{controls}} \times \text{asset value}$$

# Mobile attack vectors



Package Name "com.king.candycrushsaga"

83 items

Is Malware? Yes

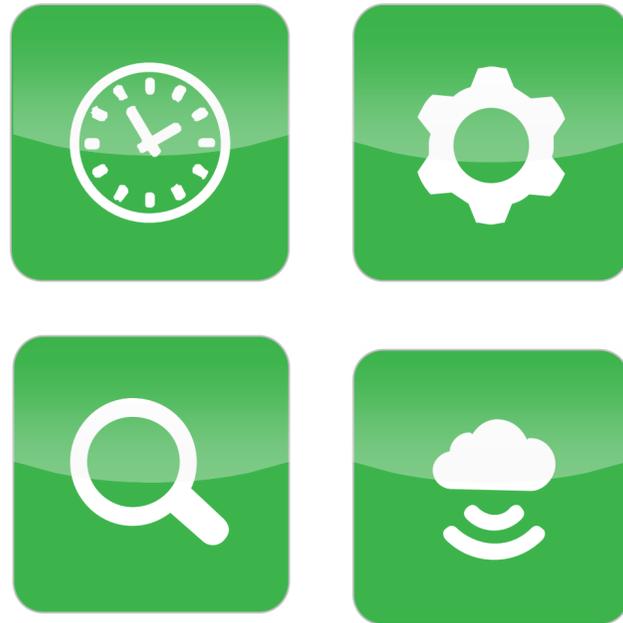
20 items

+ ADD FILTER ↓ DOWNLOAD RESULTS

< 1 / 1 >

	PACKAGE NAME	SIGNATURE	POPULARITY	SYSTEM INSTALLS	APP NAME	VERSION	THREATS
7	com.king.candycrushsaga	44c5e69d1723...	0.01598%	0.26643%	Candy Crush Saga +1	6 VERSIONS	
2	com.king.candycrushsaga	d2d96fb33665...	Very Rare	-	Candy Crush Saga	101311 1.13.1	Chargeware
3	com.king.candycrushsaga	d2009d5c93b5...	Very Rare	-	Candy Crush Saga	2 VERSIONS	Adware
5	com.king.candycrushsaga	3579b366ea0e...	Very Rare	-	Candy Crush Saga	4 VERSIONS	Adware
	com.king.candycrushsaga	643511d8e517...	Very Rare	-	Candy Crush Saga	102901100 1.2...	Adware, Trojan
4	com.king.candycrushsaga	d087a267780e...	Very Rare	-	Candy Crush Saga	101311 1.13.1	Adware
	com.king.candycrushsaga	cd6bfc17d92d...	Very Rare	-	Candy Crush Saga	101311 1.13.1	Adware, Trojan
	com.king.candycrushsaga	5e10b3ae3c99...	Very Rare	-	Candy Crush Saga	101311 1.13.1	Adware, Trojan
	com.king.candycrushsaga	be73244ad3a3...	Very Rare	-	Candy Crush Saga	101311 1.13.1	Chargeware
2	com.king.candycrushsaga	a96f15553825...	Very Rare	-	Candy Crush Saga	2 VERSIONS	Chargeware
	com.king.candycrushsaga	733848ee7e4e...	Very Rare	-	Candy Crush Saga	101201 1.12.0	Adware, Chargeware
	com.king.candycrushsaga	dffaa0df699e1...	Very Rare	-	Candy Crush Saga	1 1.56.0.3	Adware

- App behavior risk spectrum



Exhibits no sensitive behaviors



Exhibits one or more sensitive behaviors



Exhibits malicious behaviors

# 3<sup>rd</sup> Party App Analysis

Understand the capabilities and risky behaviors of the apps on your employees' mobile devices

The screenshot shows the Lookout mobile application interface. On the left is a dark sidebar with the Lookout logo and navigation options: Dashboard, Reports, Threats, Apps (highlighted), Devices, Policy, Settings, and Support. The main content area is titled 'Facebook Messenger' and includes a 'BLACKLIST' button in the top right. Below the title is a table with the following data:

DEVELOPER	OS	VERSION	FILE SIZE	YOUR FLEET
Facebook	Apple	1.3.5	128MB	18% of devices

Below the table is an 'Identification' section with a Messenger icon and the following details:

- Bundle ID: com.facebook.katana.msg
- Team ID: 4FP24NRQW2
- File Hash: cacb392b1bc43dcd2d9733b7415385c5a8cd0cc6

The 'Description' section contains the following text:

Instantly reach the people in your life—for free. Messenger is just like texting, but you don't have to pay for every message (it works with your data plan).

Not just for Facebook friends: Message people in your phone book and just enter a phone number to add a new contact.

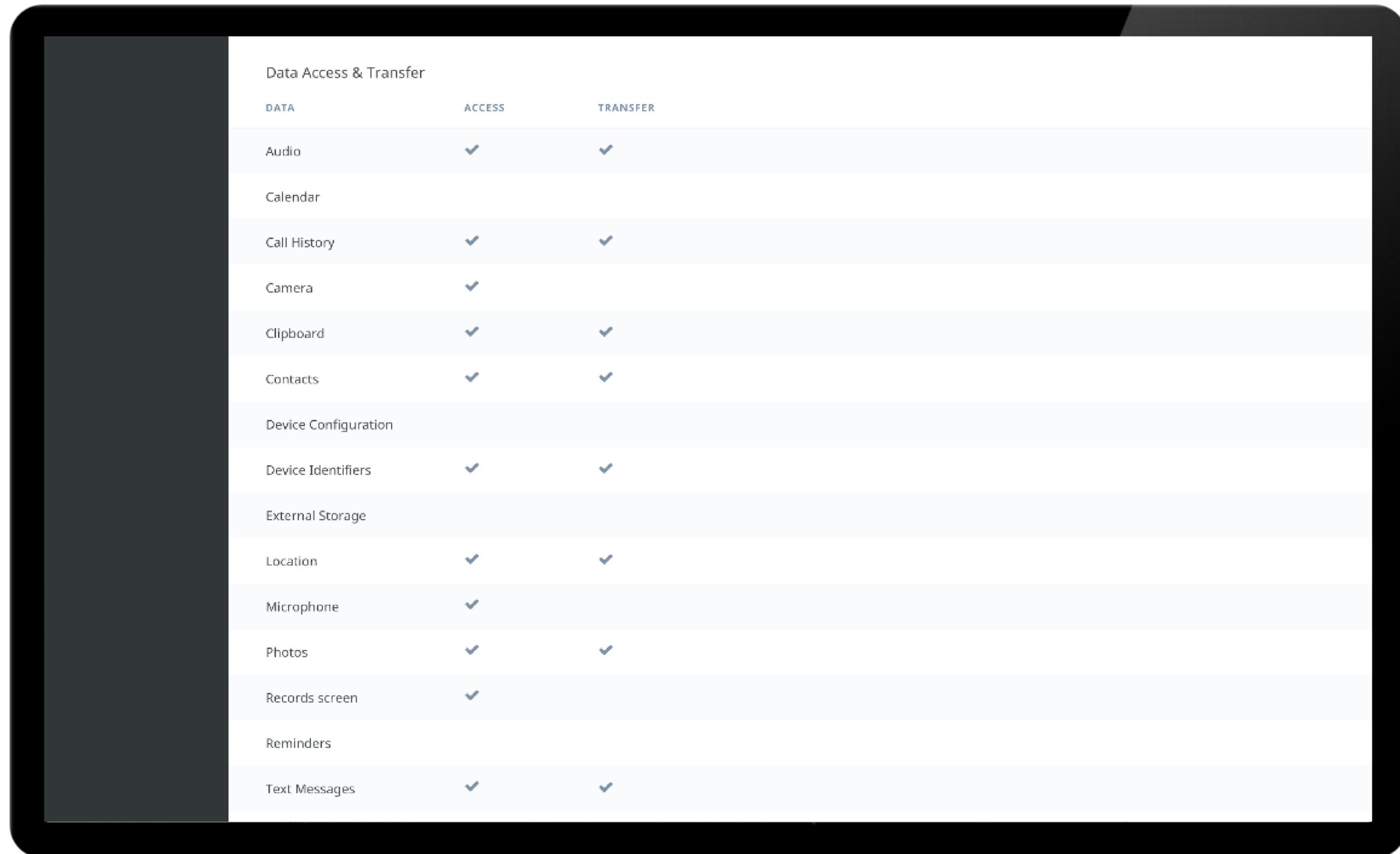
Group chats: Create groups for the people you message most. Name them, set group photos and keep them all in one place.

Photos and videos: Shoot videos and snap selfies or other photos right from the app and

The 'Malware' section at the bottom states: 'No malware detected'.

# 3<sup>rd</sup> Party App Analysis

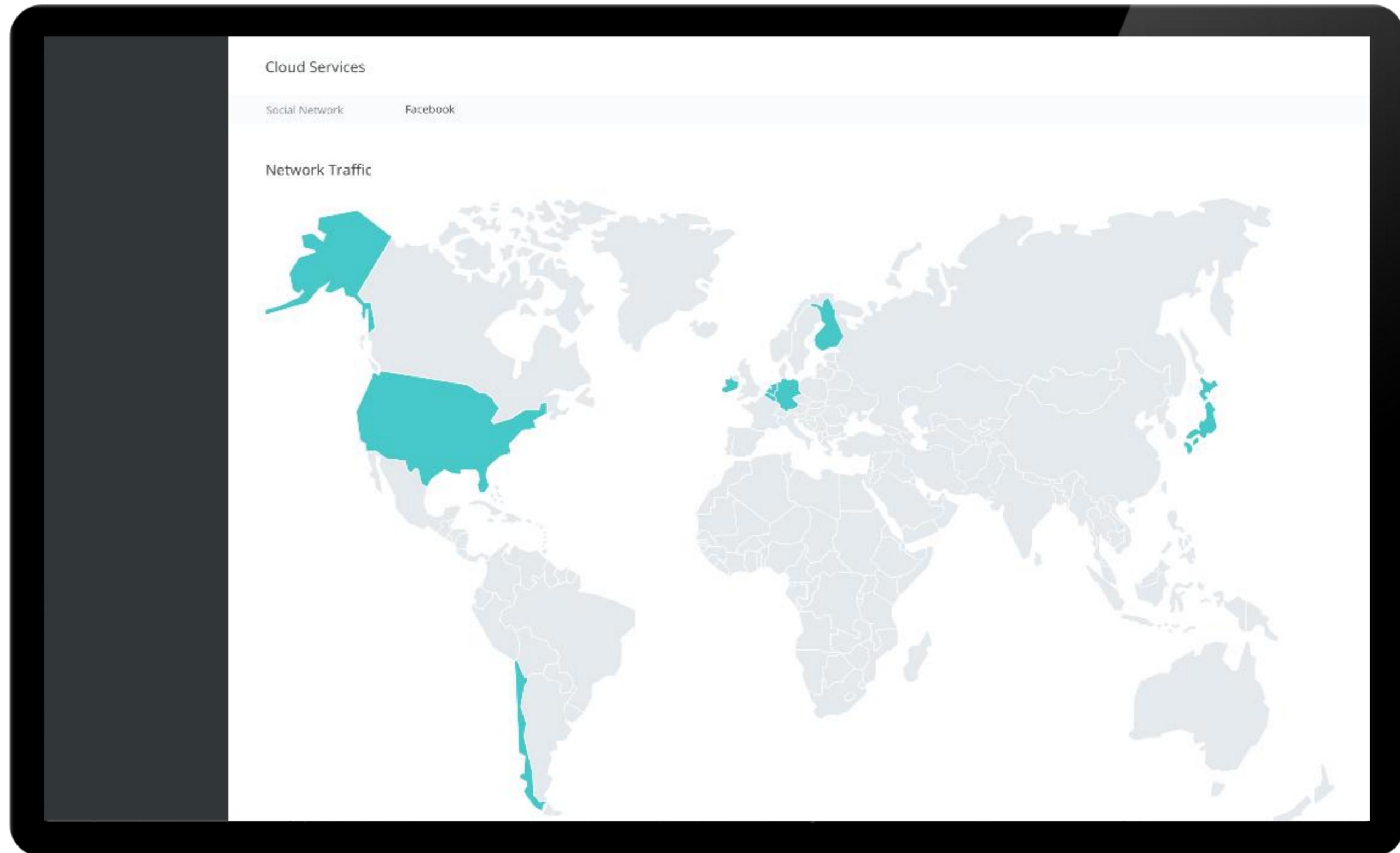
Understand the capabilities and risky behaviors of the apps on your employees' mobile devices



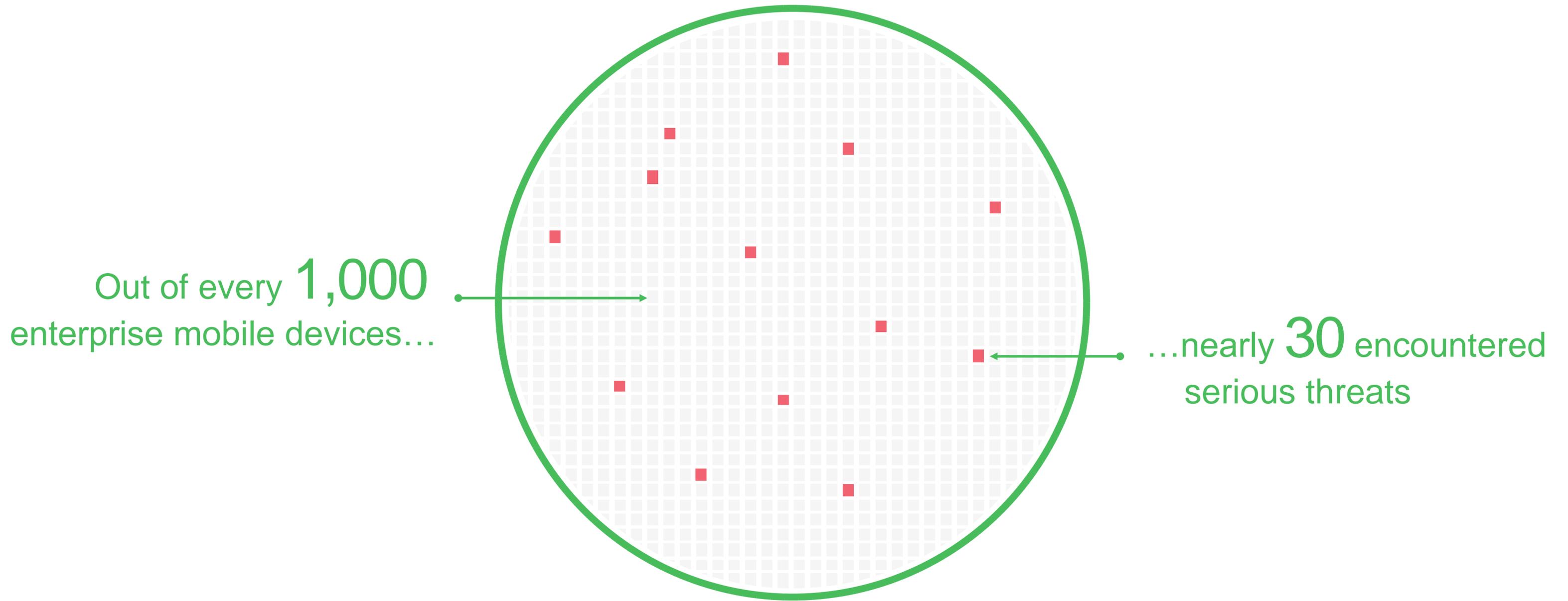
Data Access & Transfer		
DATA	ACCESS	TRANSFER
Audio	✓	✓
Calendar		
Call History	✓	✓
Camera	✓	
Clipboard	✓	✓
Contacts	✓	✓
Device Configuration		
Device Identifiers	✓	✓
External Storage		
Location	✓	✓
Microphone	✓	
Photos	✓	✓
Records screen	✓	
Reminders		
Text Messages	✓	✓

# 3<sup>rd</sup> Party App Analysis

Understand the capabilities and risky behaviors of the apps on your employees' mobile devices

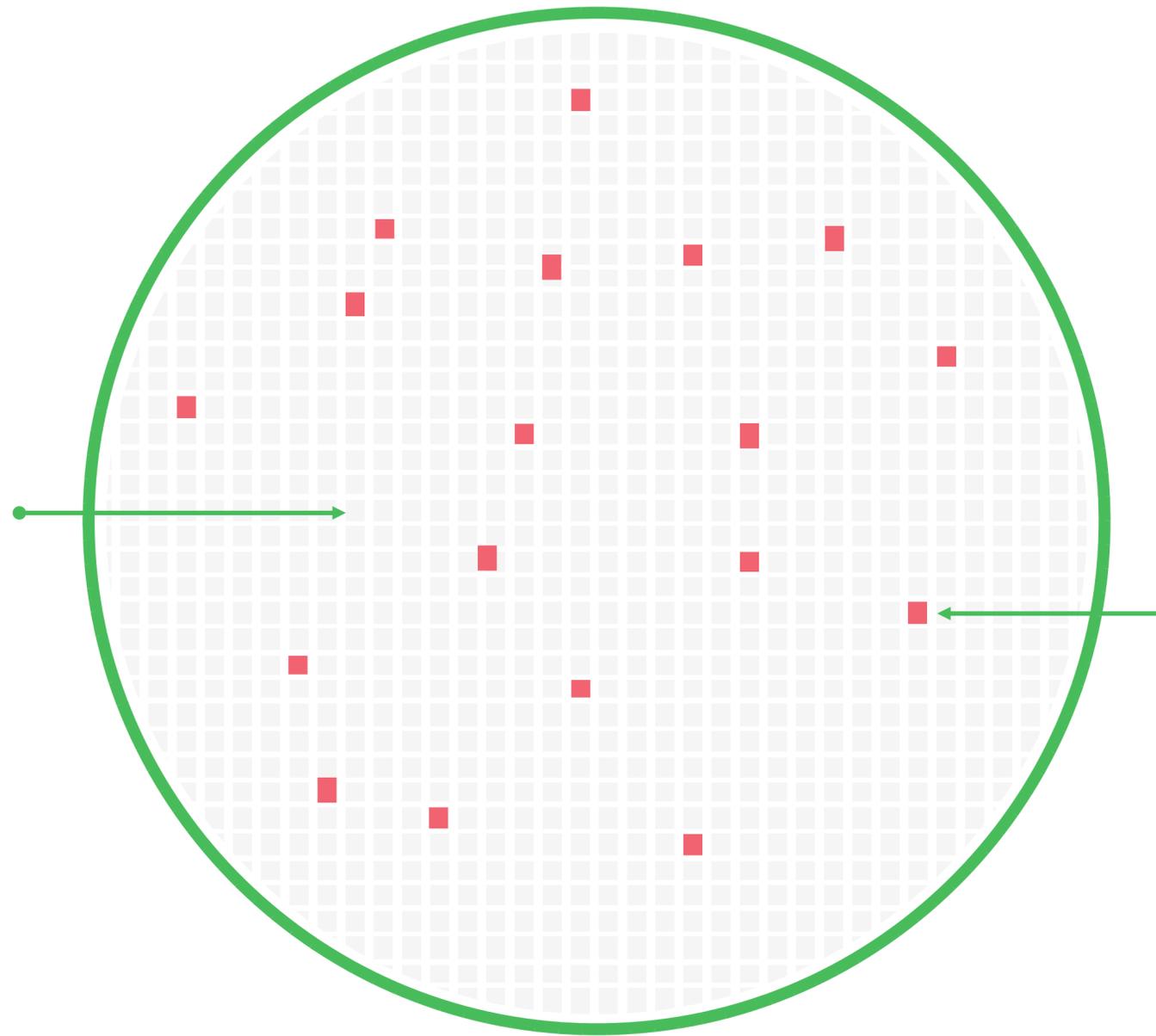


# General threat encounter rate for enterprise mobile devices



# Threat encounter rate for Retail Sector mobile devices

Out of every **1,000**  
enterprise mobile devices...



... **45** serious threats,  
of which

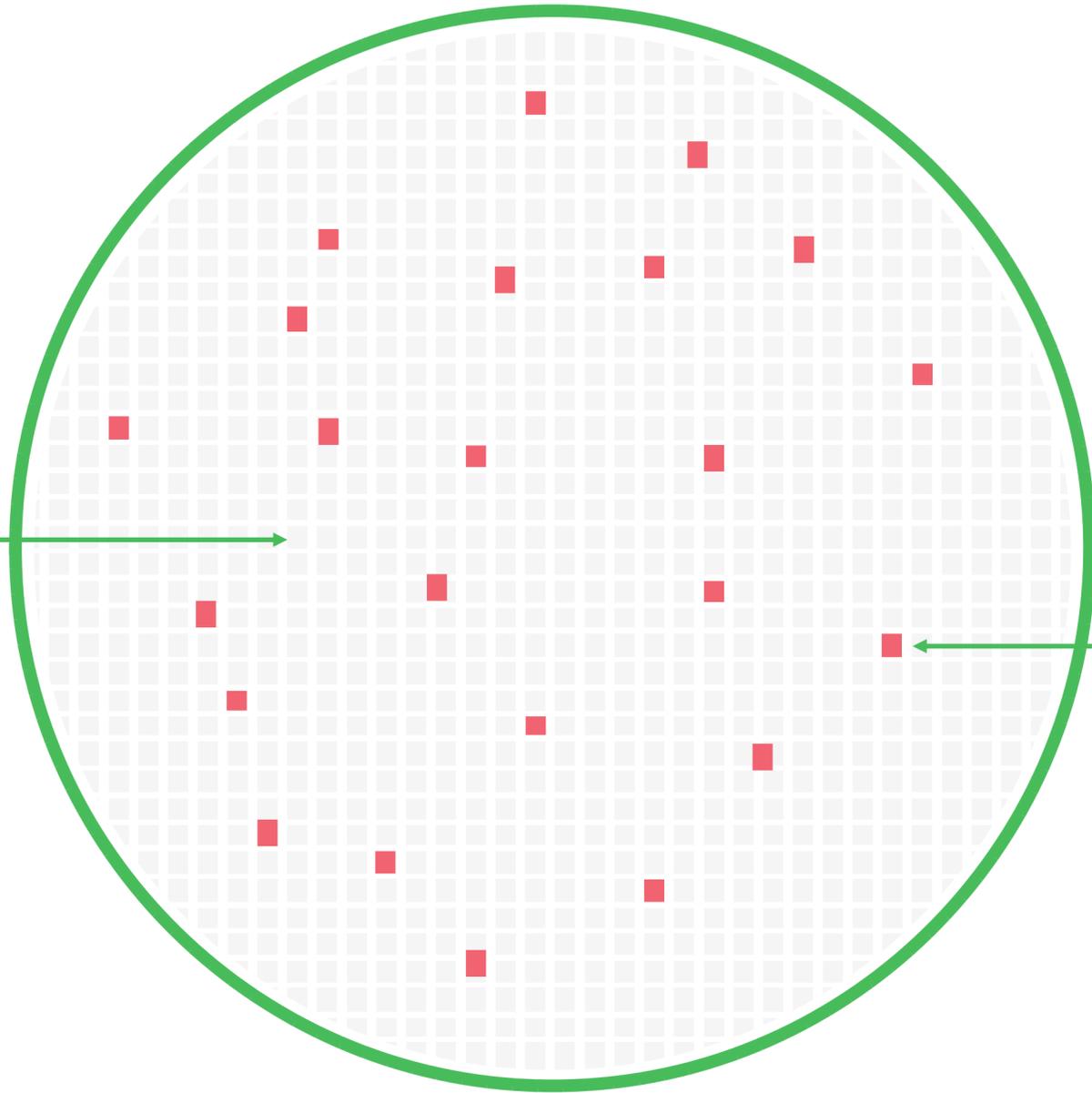
... **32** trojans

... **7** root enablers

... **4** surveillance

# Threat encounter rate for Healthcare mobile devices

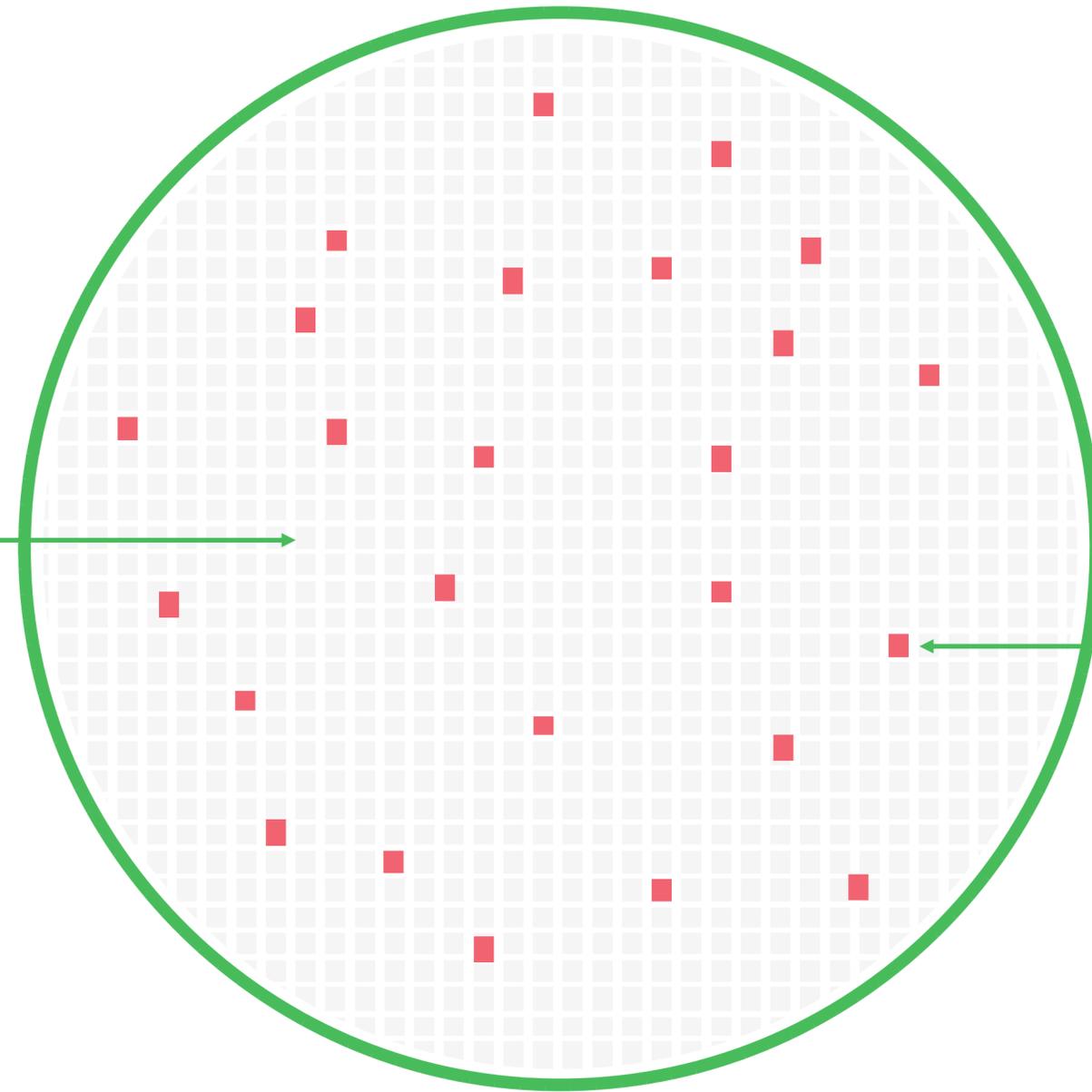
Out of every **1,000** enterprise mobile devices...



... **67** serious threats,  
of which  
... **42** trojans  
... **14** root enablers  
... **7** surveillance

# Threat encounter rate for Financial Sector mobile devices

Out of every **1,000** enterprise mobile devices...



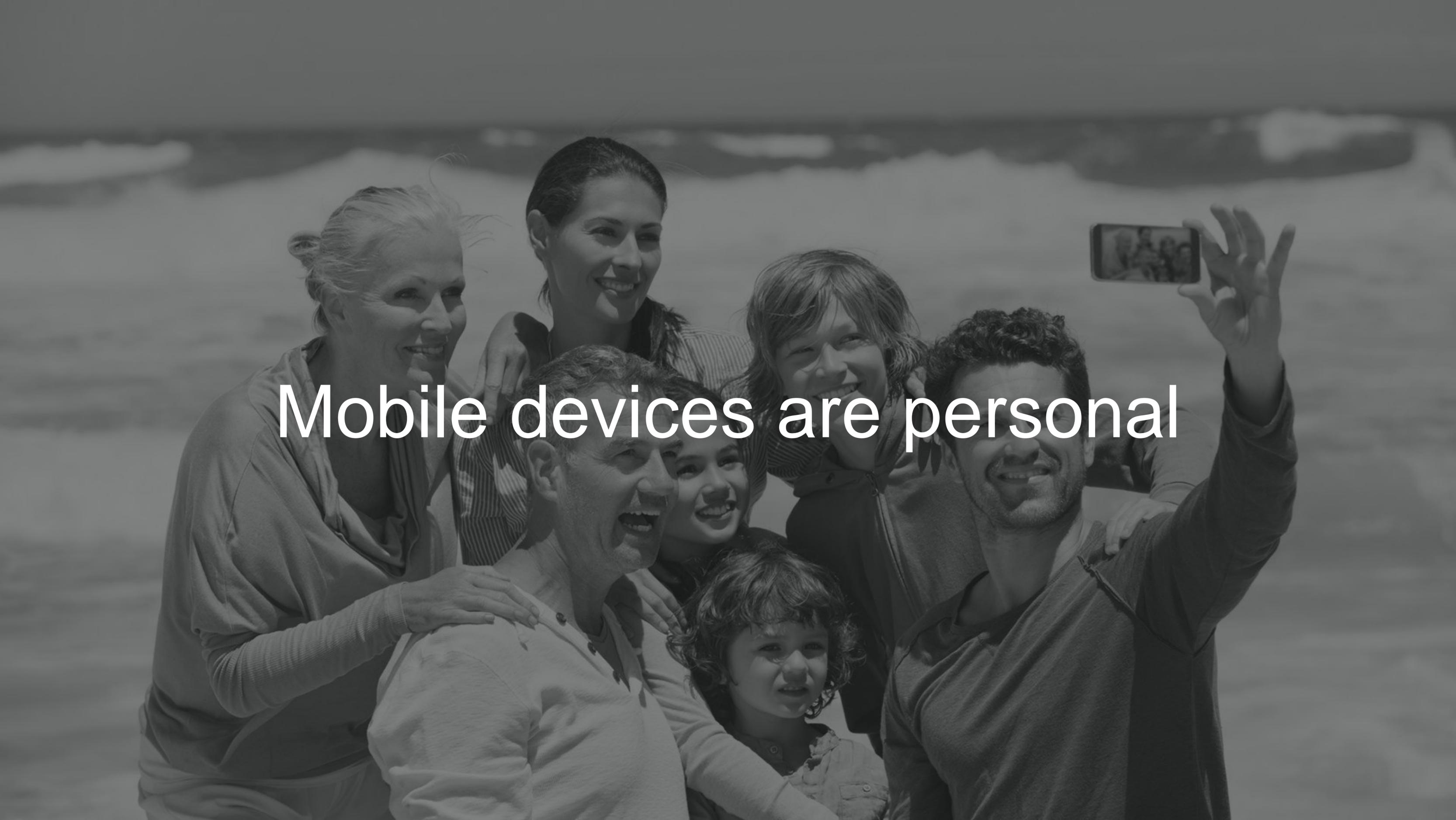
... **70** serious threats,  
of which  
... **42** trojans  
... **14** root enablers  
... **8** surveillance

$$\frac{\text{threats} \times \text{vulnerabilities}}{\text{controls}} \times \text{asset value}$$

## GDPR Principal #6:

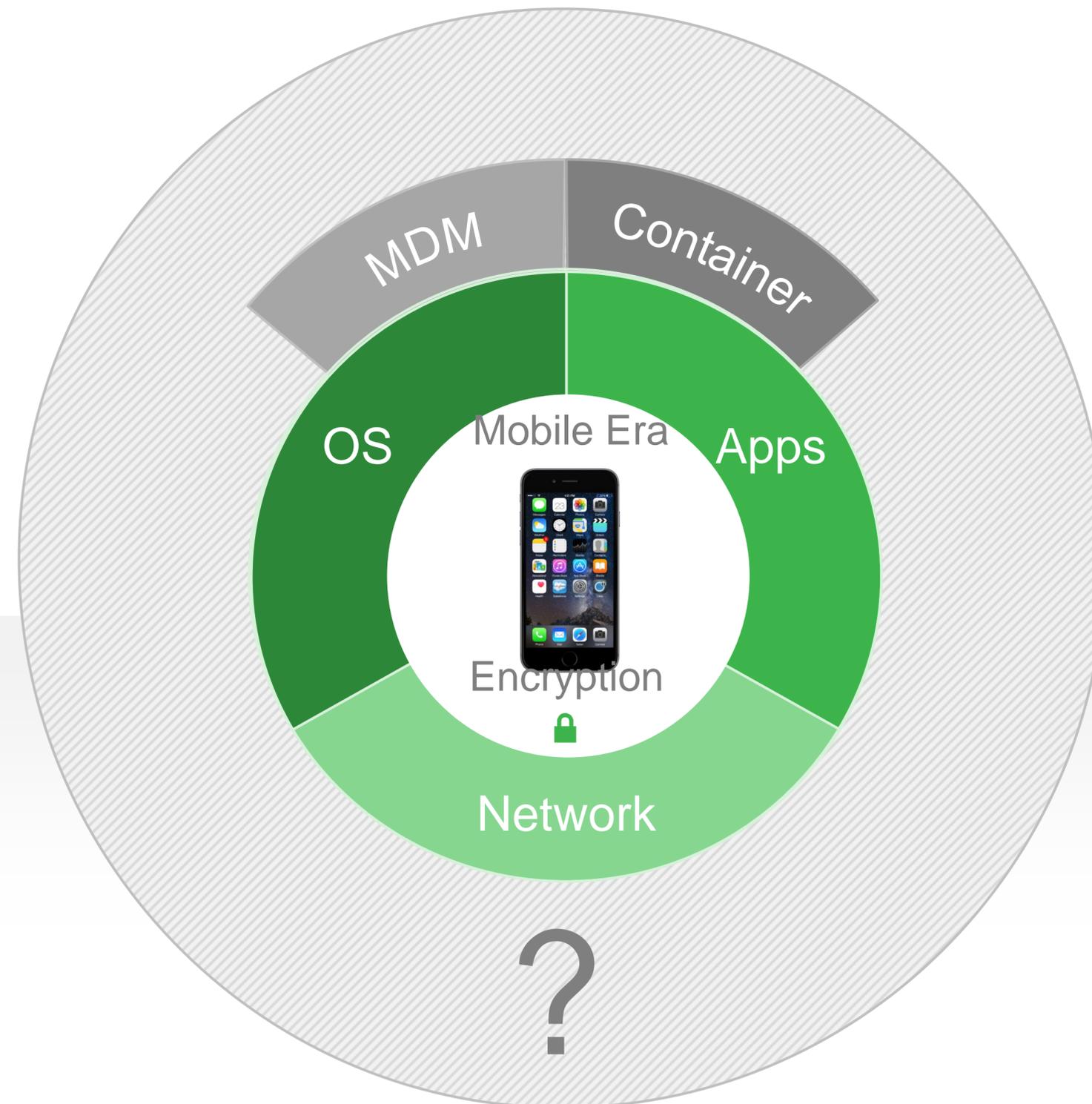
Personal data shall be....

processed in a manner that **ensures appropriate security of the personal data**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate **technical or organisational measures**.



Mobile devices are personal

Encrypt, contain and control as first steps.



# EMM + Security

vmware® airwatch®

Microsoft Intune

MobileIron

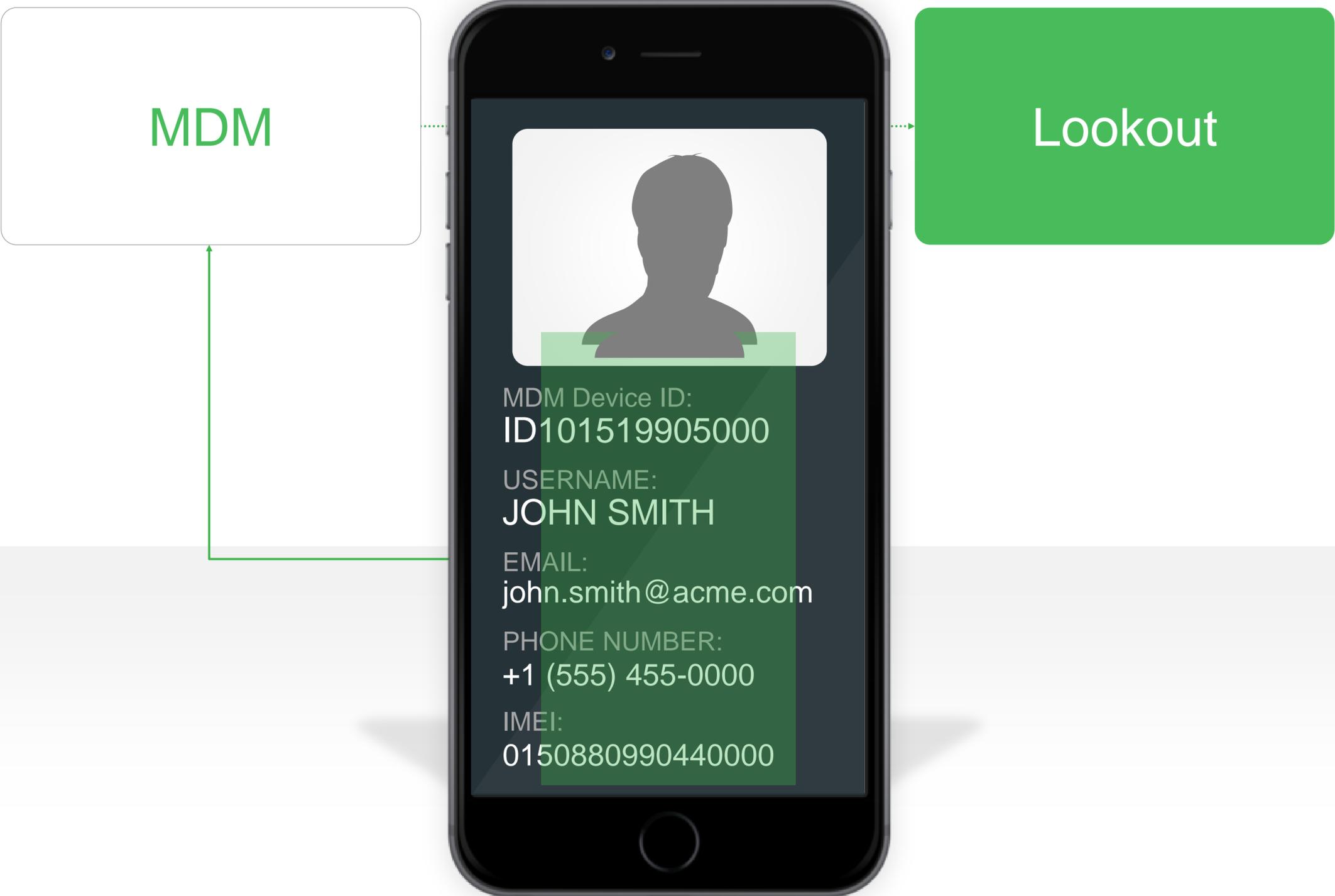
MaaS360®  
by Fiberlink, an IBM company



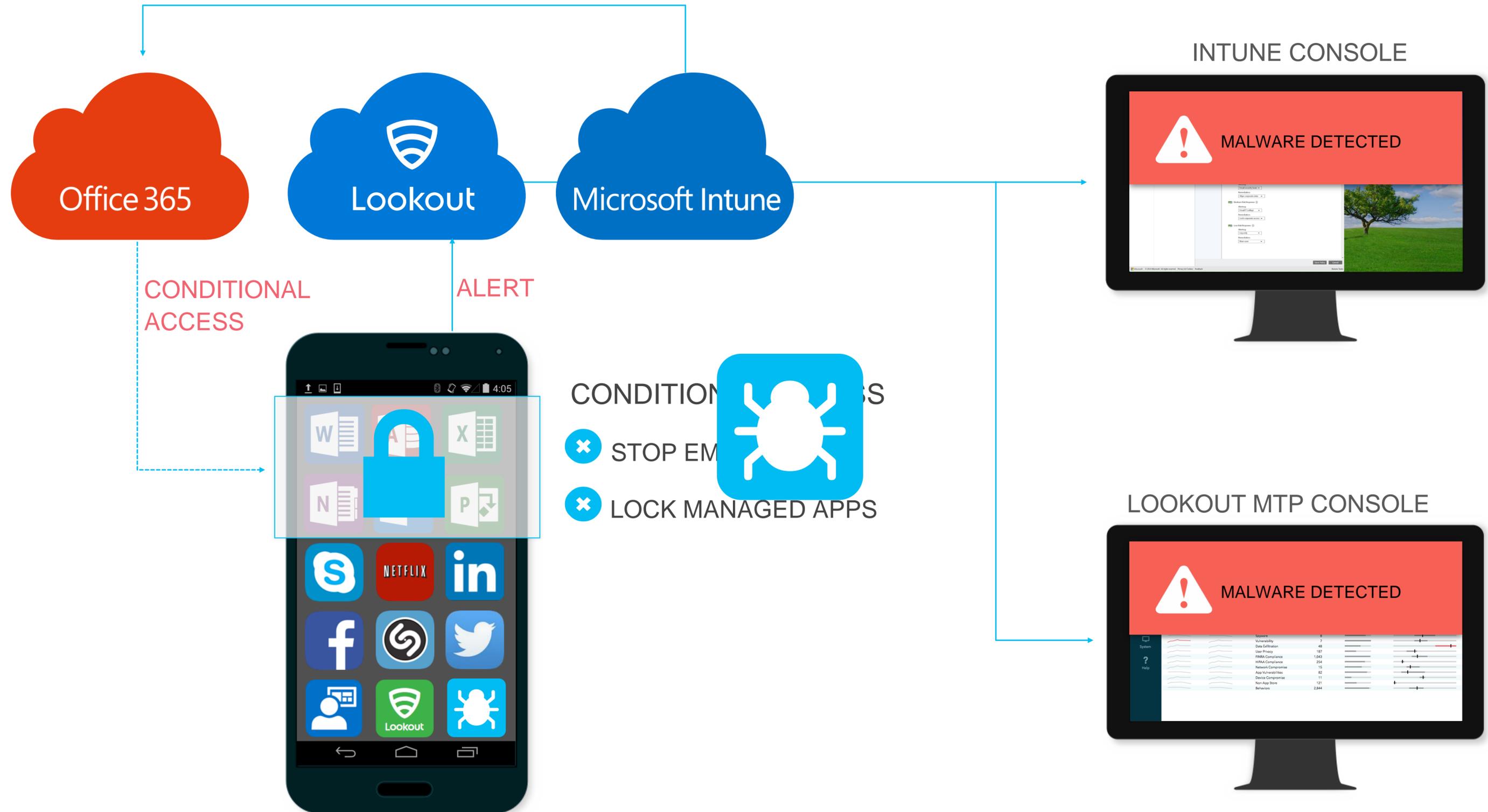
RISKS	EMM ONLY	SECURITY + EMM
Lost Device	✓ Protected	✓ Protected
App distribution	✓ Protected	✓ Protected
Policy violations	! Limited Protection	✓ Protected
Data leakage	! Limited Protection	✓ Protected
Jailbreaking & rooting	! Limited Protection	✓ Protected
Malicious apps	x No Protection	✓ Protected
Container exploits	x No Protection	✓ Protected
Network attacks	x No Protection	✓ Protected

# Privacy by design:

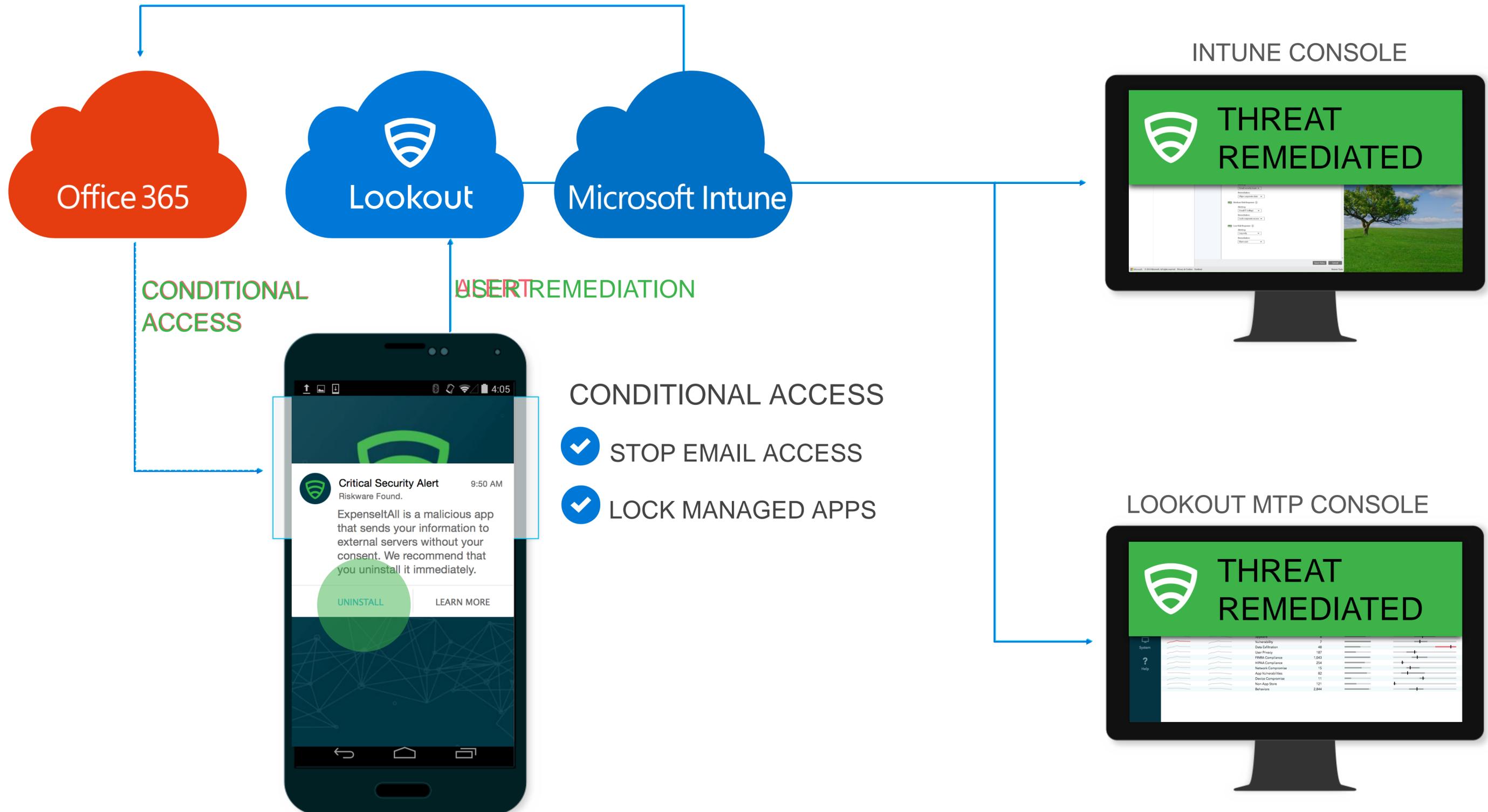
## Data privacy controls limit what Lookout can see



# APP-BASED THREAT TRIGGERS CONDITIONAL ACCESS TO O365



# APP-BASED THREAT TRIGGERS CONDITIONAL ACCESS TO O365



# Healthcare Case Study



CASE STUDY

## Buurtzorg protects healthcare data by securing 8K iPads



### The Challenge

Buurtzorg Nederland (Buurtzorg) home care nurses spend the vast majority of their time traveling to visit patients and serving them in their homes. These nurses use company-owned iPads, managed with MobileIron Enterprise Mobility Management (EMM), as their main productivity tool.

The fleet of iPads give the nurses access to sensitive patient information such as nursing assessments and billing through Buurtzorg's own app. The caretakers also frequently use public Wi-Fi connections to access apps that assist them in daily tasks like evaluating injuries. These use cases created a challenge for leaders at Buurtzorg. They wanted employees to freely use their iPads in the most productive way, but also felt they had to establish and manage policies for acceptable apps in order to protect patient data.

“Blacklisting apps is very difficult because there are a lot of apps in the App Store and if we whitelist apps, employees don't have very much freedom anymore.”

**Jos de Blok**, CEO and co-founder



### Customer Profile

Buurtzorg Nederland is a Dutch home health care organization renowned for its use of self-governing teams of nurses to deliver high-quality care. The company's name is Dutch for "neighborhood care."

**Industry:** Healthcare

**Mobility Policy:** COPE

### The Solution

Lookout Mobile Endpoint Security

### The Results

- 100% mobile threat remediation, completed by non-technical users
- Improved productivity for remote nurse teams
- Gained compliance with Dutch privacy laws regarding the security of private data on mobile devices
- Achieved visibility into network and app-based mobile threats with the potential to cause data loss

- Industry: Healthcare
- Device Policy: COPE
- MDM: MobileIron

### Results:

- Improved productivity for remote nursing teams
- 100% mobile threat remediation by non-technical users
- Gained compliance with Dutch privacy laws regarding private data on mobile devices
- Visibility into network and app-based threats with potential to cause data loss

You don't have visibility yet, but we do.



## Mobile Risk Assessment Report for Anonymized

Prepared by Nick Fisher Jul 13, 2015 5:54:55 PM

### Anonymized



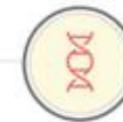
195

Devices and accounts on your network.



59

App-based threats encountered.



21

Threat families encountered.



**EVERYTHING WILL BE OK**