



GPDR & Mobility : Securing Mobile

Tom Davison, EMEA SE Mgr | Friday 3rd 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 long-sleeved shirt and a watch on their left wrist. In the background, a dark-colored laptop bag with multiple straps and buckles is visible. A small, light-colored label with the word "Herschel" is attached to one of the straps. The overall image has a muted, dark tone.

Phones, tablets, and wearables have replaced managed laptops.



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

A grayscale photograph of a person's hand covering their face, with fingers spread, suggesting a gesture of despair, frustration, or a lack of control. The background is dark and out of focus.

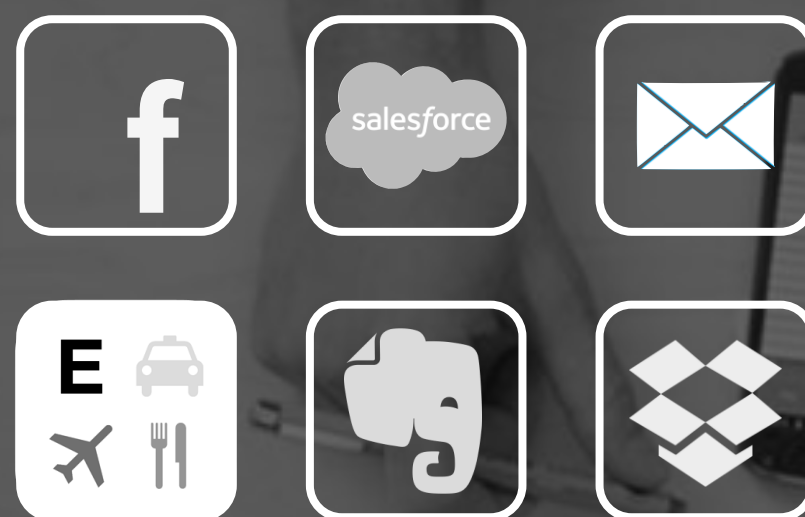
The new world of choice puts
your data in the hands of users,
and out of your control.



51%

Time on mobile, vs
42% on PC

KPCB | KLEINER
PERKINS
CAUFIELD
BYERS



90%

Time in apps,
not the browser.



OS and form factors are
converging



Risk =

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

Consider the data on you mobile device

ENTERPRISE EMAIL

CREDENTIALS
Stored, Soft Tokens

ENTERPRISE NETWORK
VPN, WiFi

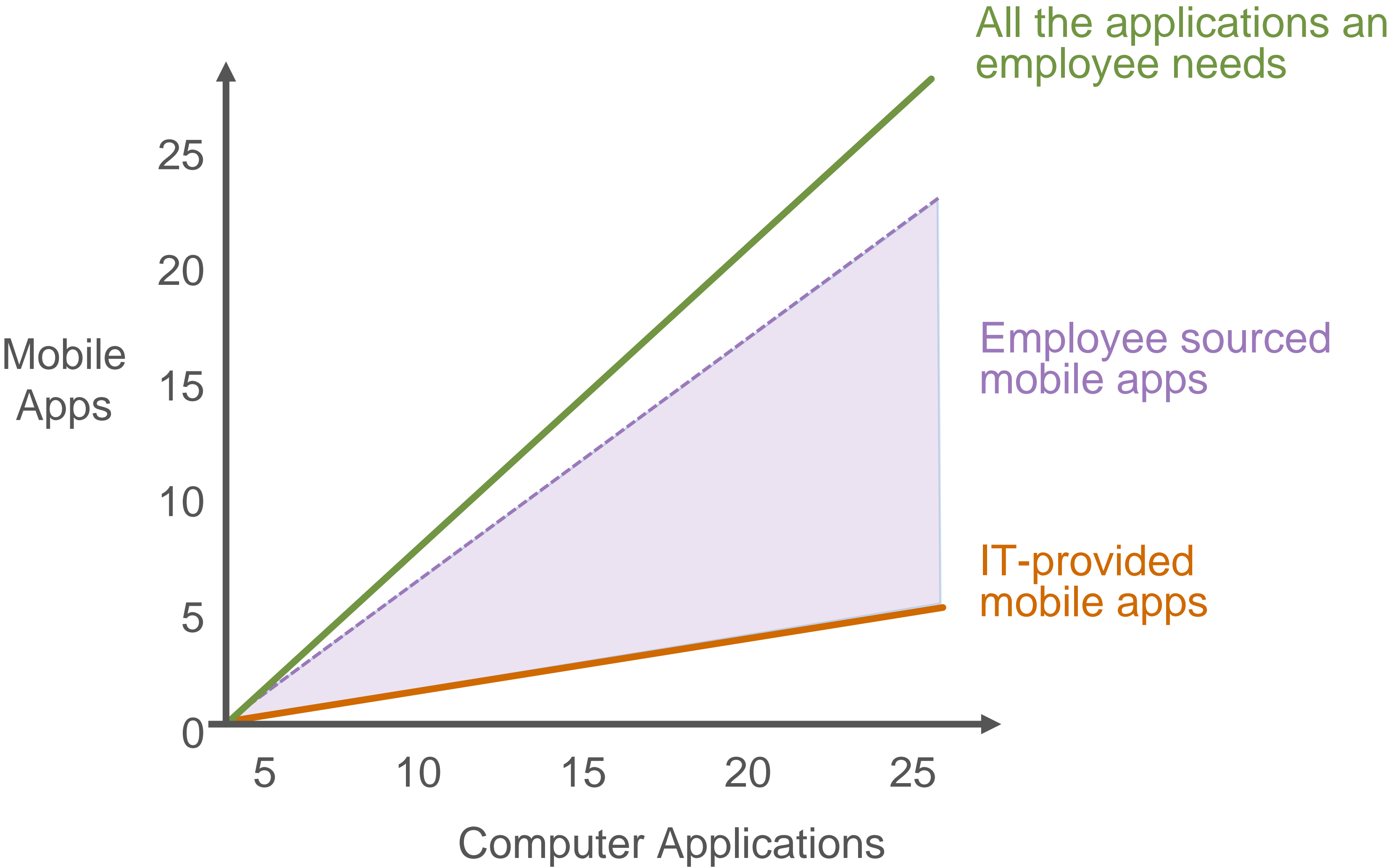
ENTERPRISE APPS
SaaS, Custom Apps

PHOTO ALBUM
Whiteboard Screenshots, IDs

SENSORS
GPS, Microphone, Camera



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)




<h3>Opportunity</h3> <p>120k users</p> <p>14k apps</p>	<h3>Forecast</h3> <p>80%</p> <p>60%</p>	<p>Mon Oct-14, 10:32am Bob to assign Director (Kevin?) to project and provide requirements.</p> <p>Thu Oct-10 9:12am Bob said he is unlikely to get budget for this project, but will find out more in planning...</p>	New Edit Edit
<h3>History</h3> <p>8.2k users</p> <p>1,600 apps</p> <p>2,000 users</p> <p>100 users</p>	<h3>SA</h3> <p>30-Jun-15</p> <p>31-Dec-14</p> <p>30-Jun-14</p> <p>30-Jun-14</p>	<h3>Details</h3> <p>BYOD project "Choice" led by Bob. Rollout staged...</p> <p>Infrastructure update to enable DR and Business...</p> <p>Initial purchase for Networking group for Project...</p> <p>Proof-of-concept purchase for Project Choice (BY...</p>	
<h3>Customer Care</h3> <p>Failed Login  Mon Oct-14, 8:15am Provided work-around for login issue...</p> <p>Appliance F...  Tue Oct-1, 3:22pm Replaced faulty NIC under warranty usi...</p>			




Customer




Opportunity



Pipeline

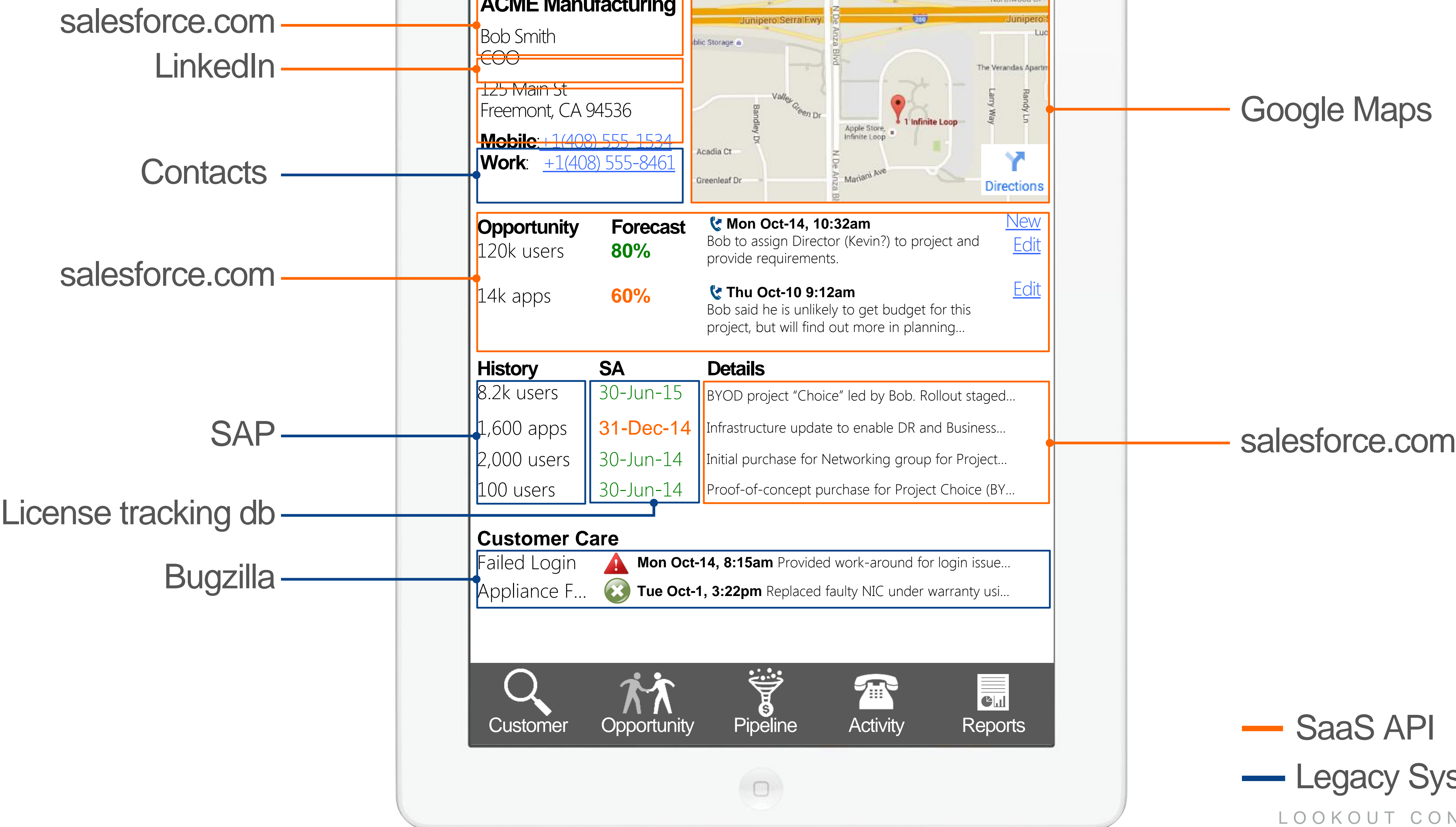


Activity



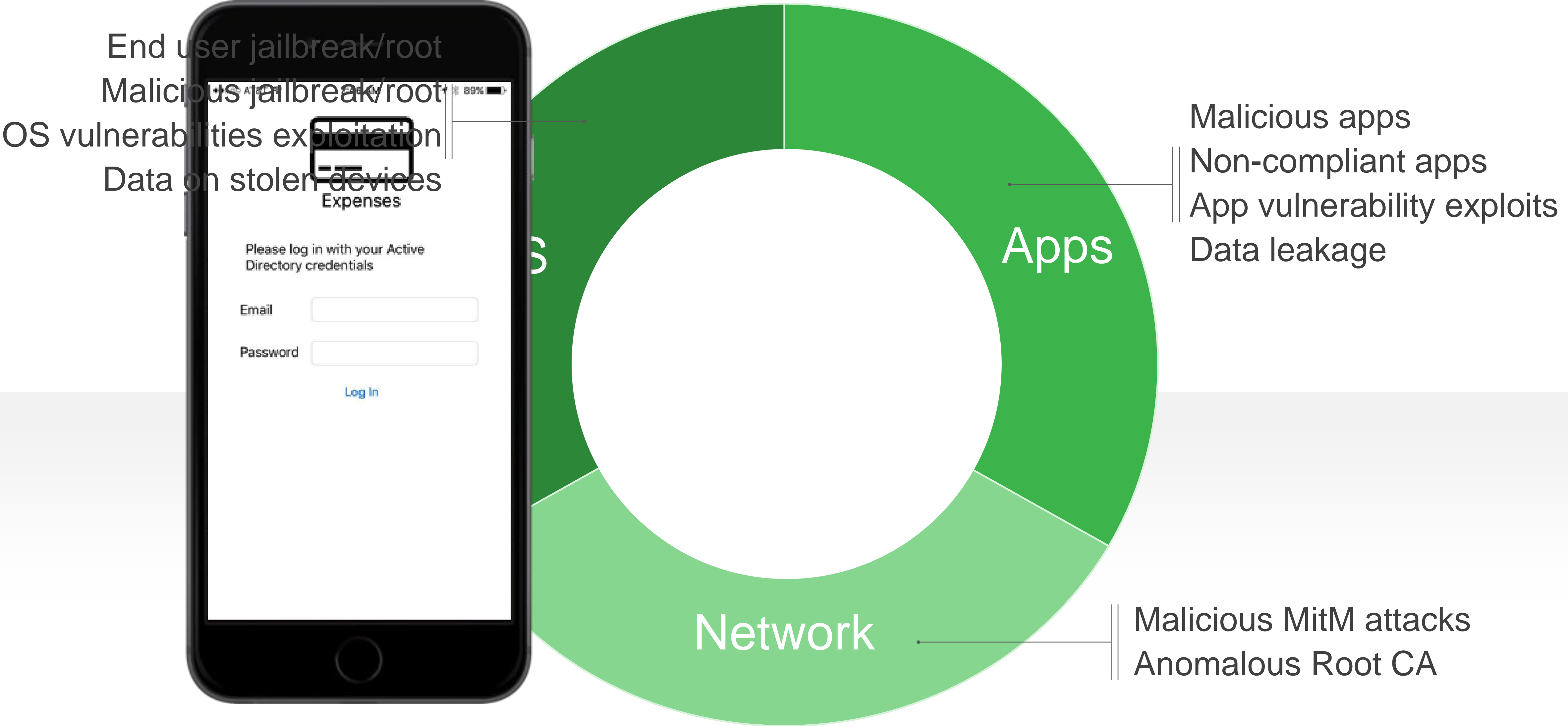
Reports

SALES MASHUP



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

Mobile attack vectors



Package Name "com.king.candycrushsaga"

83 items

Is Malware? Yes

20 items

+ ADD FILTER ↓ DOWNLOAD RESULTS

	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



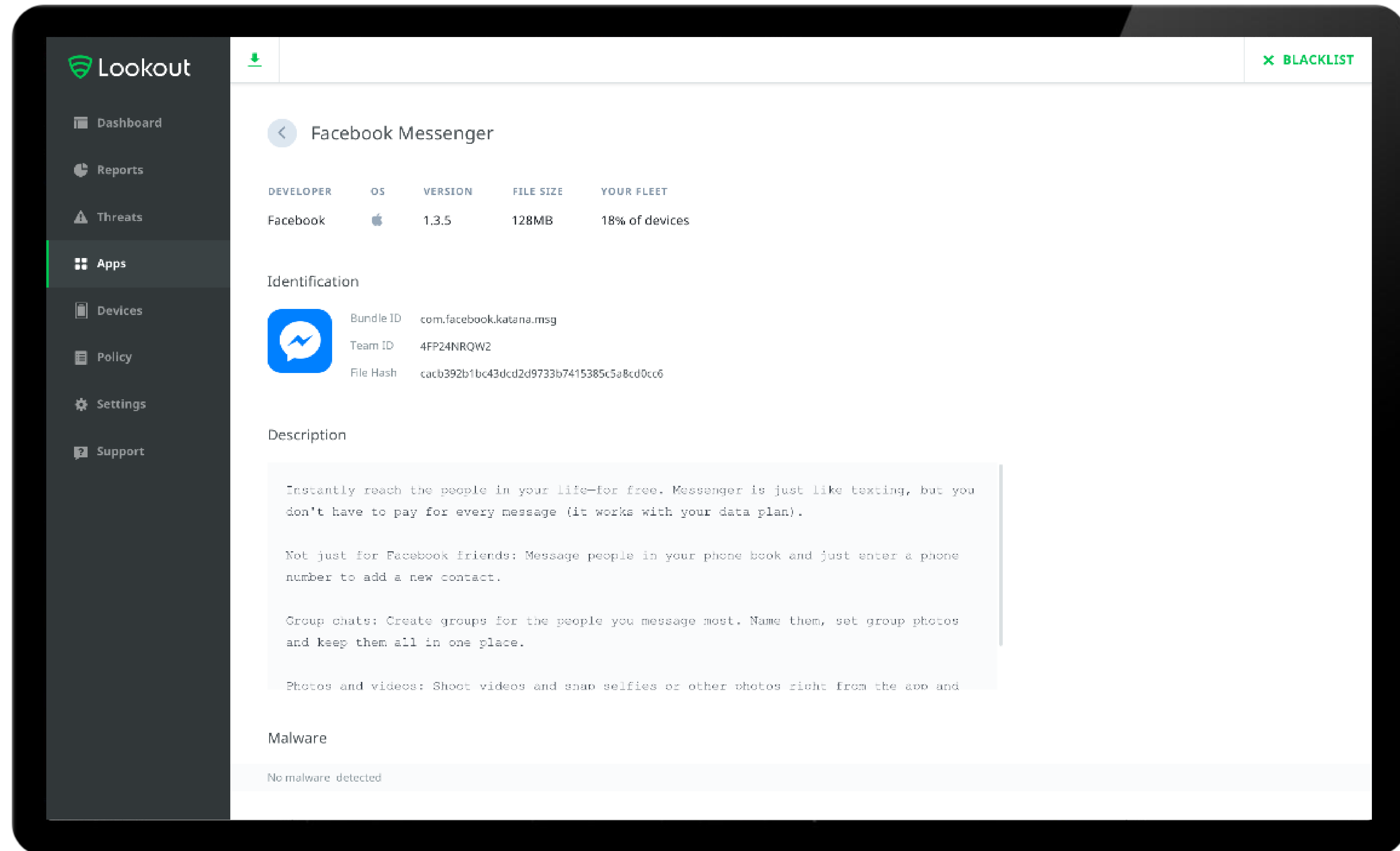
Exhibits one or more sensitive behaviors



Exhibits malicious behaviors

3rd Party App Analysis

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



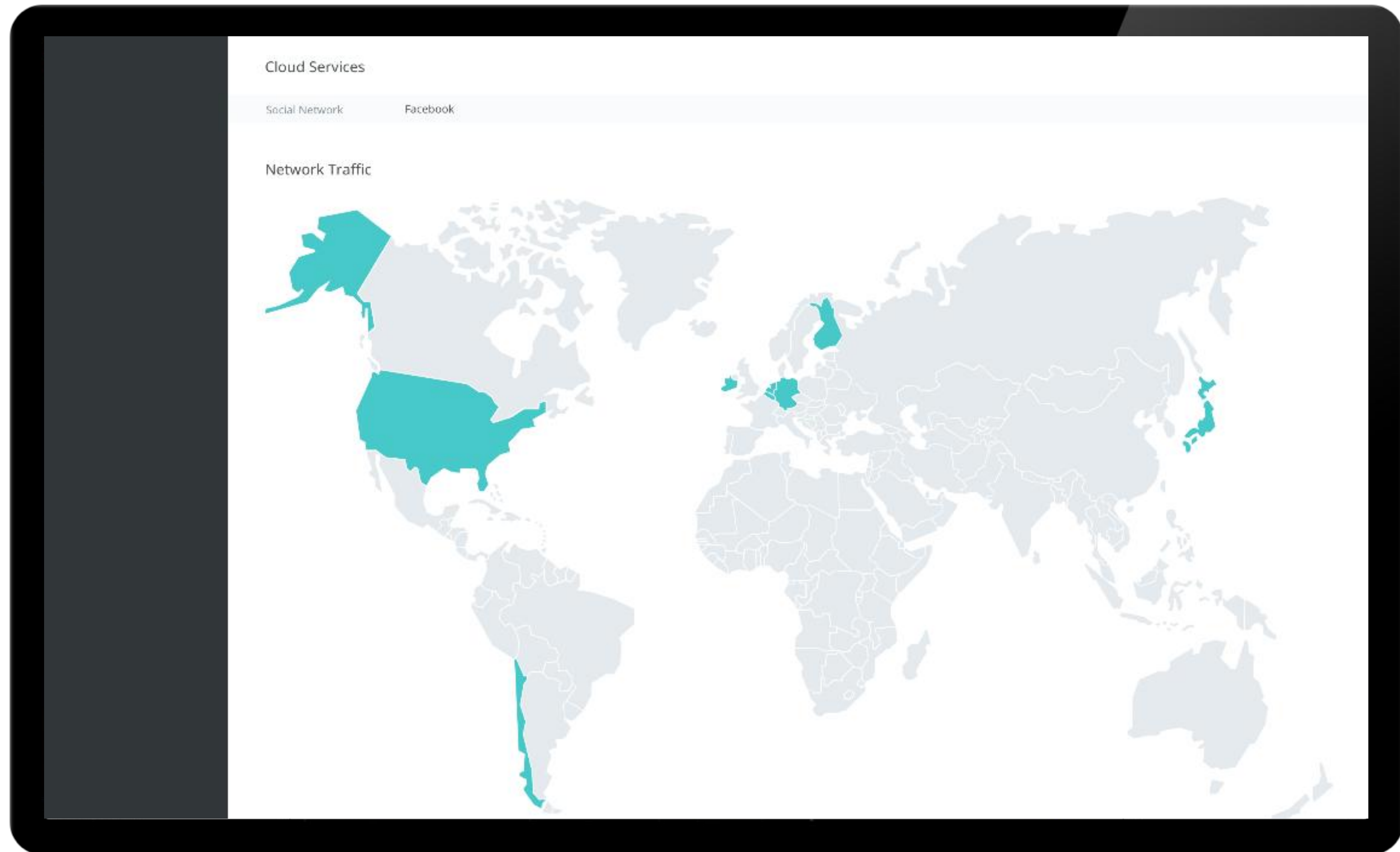
3rd Party App Analysis

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

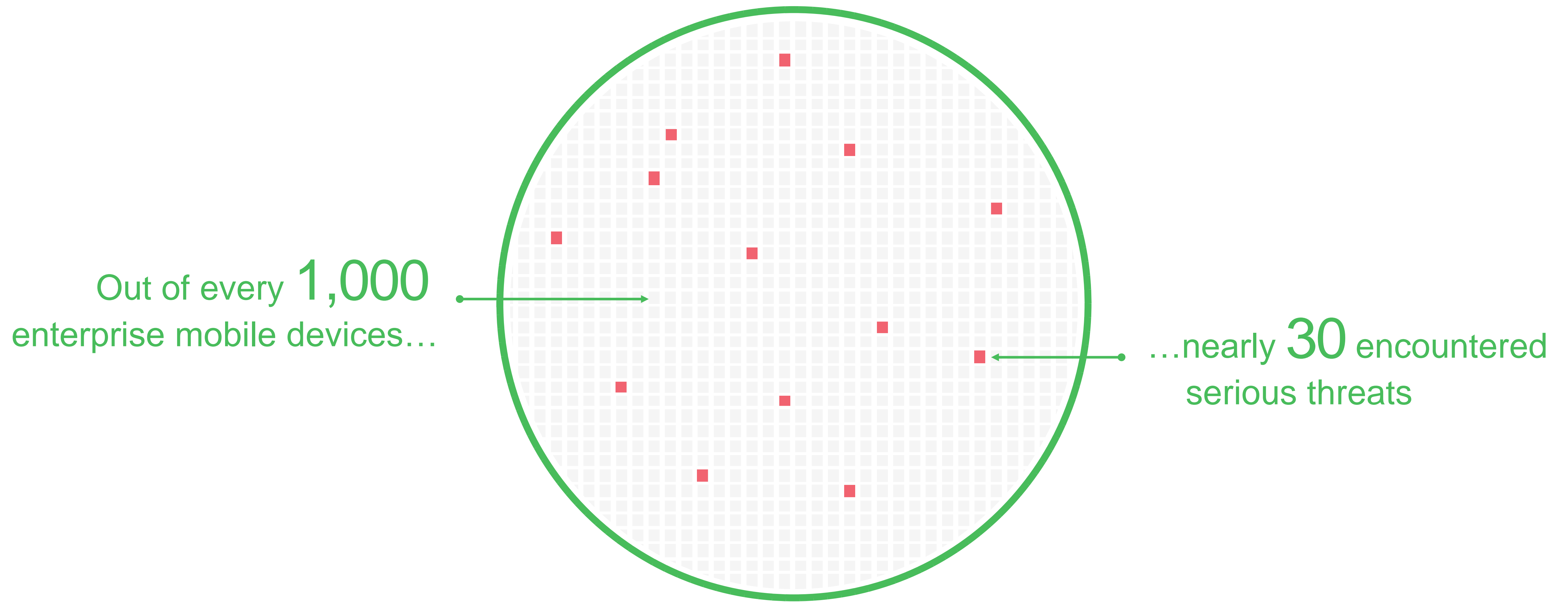
Data Access & Transfer		
DATA	ACCESS	TRANSFER
Audio	✓	✓
Calendar		
Call History	✓	✓
Camera	✓	
Clipboard	✓	✓
Contacts	✓	✓
Device Configuration		
Device Identifiers	✓	✓
External Storage		
Location	✓	✓
Microphone	✓	
Photos	✓	✓
Records screen	✓	
Reminders		
Text Messages	✓	✓

3rd Party App Analysis

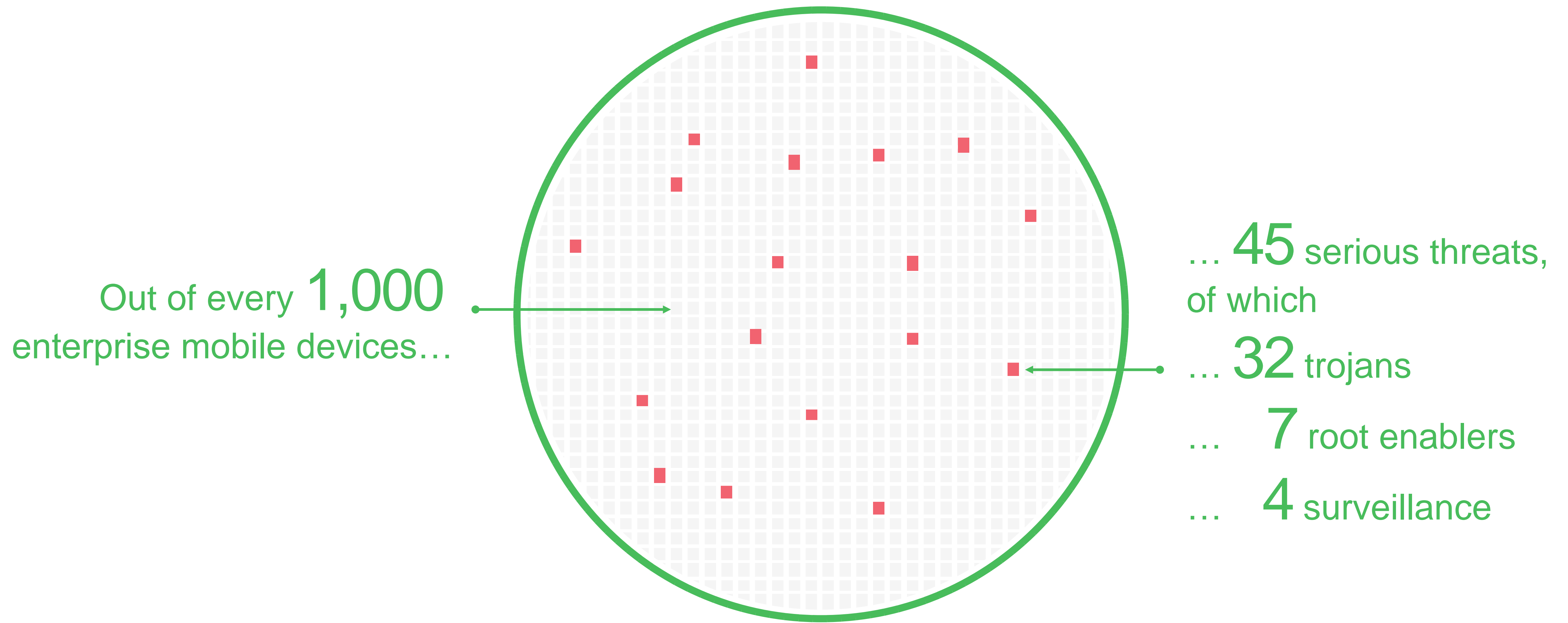
Understand the capabilities and risky behaviors of the apps on your employees' mobile devices



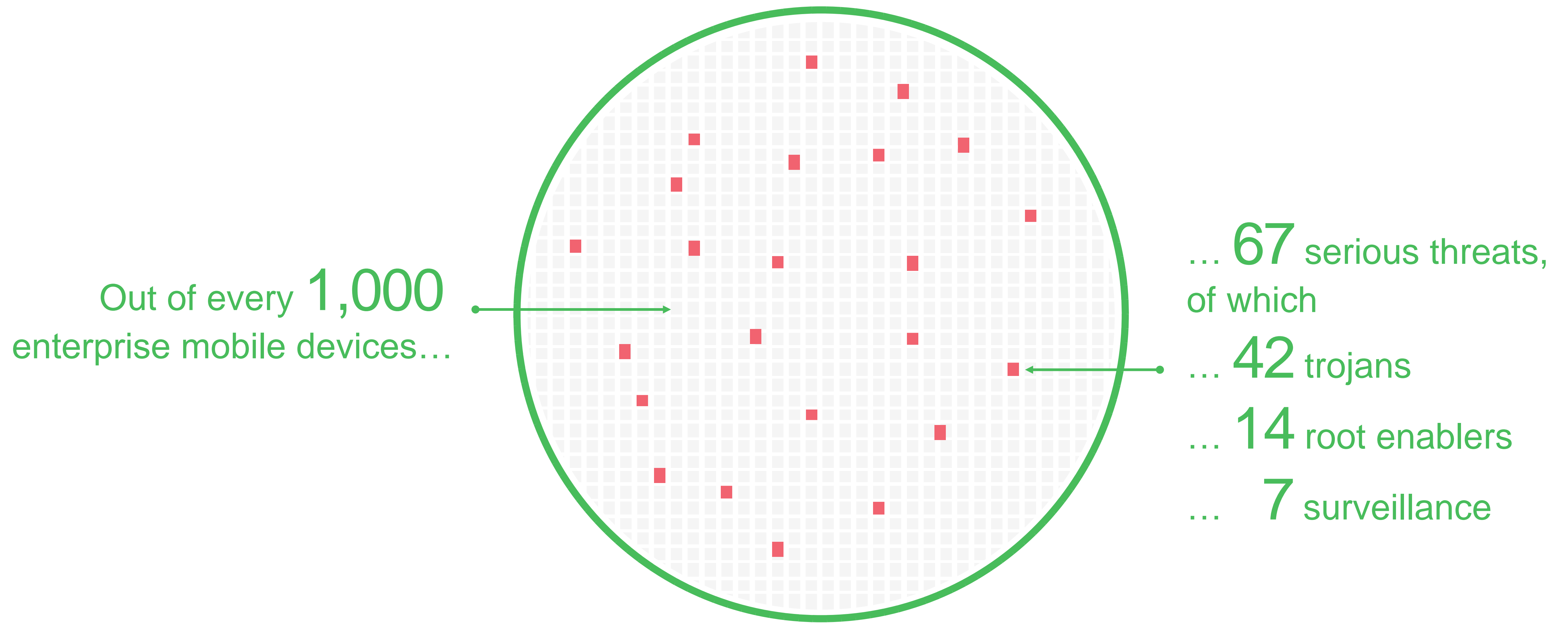
General threat encounter rate for enterprise mobile devices



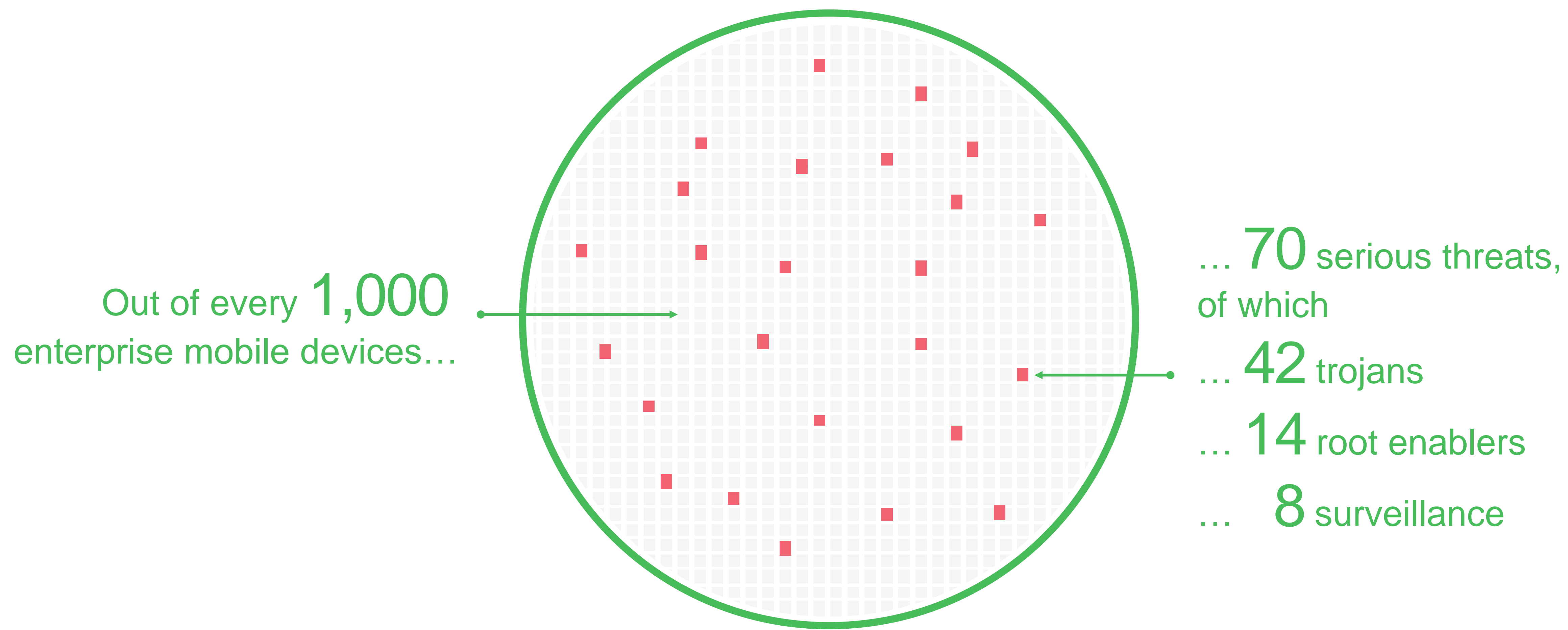
Threat encounter rate for Retail Sector mobile devices



Threat encounter rate for Healthcare mobile devices



Threat encounter rate for Financial Sector mobile devices



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

GDPR Principal #6:

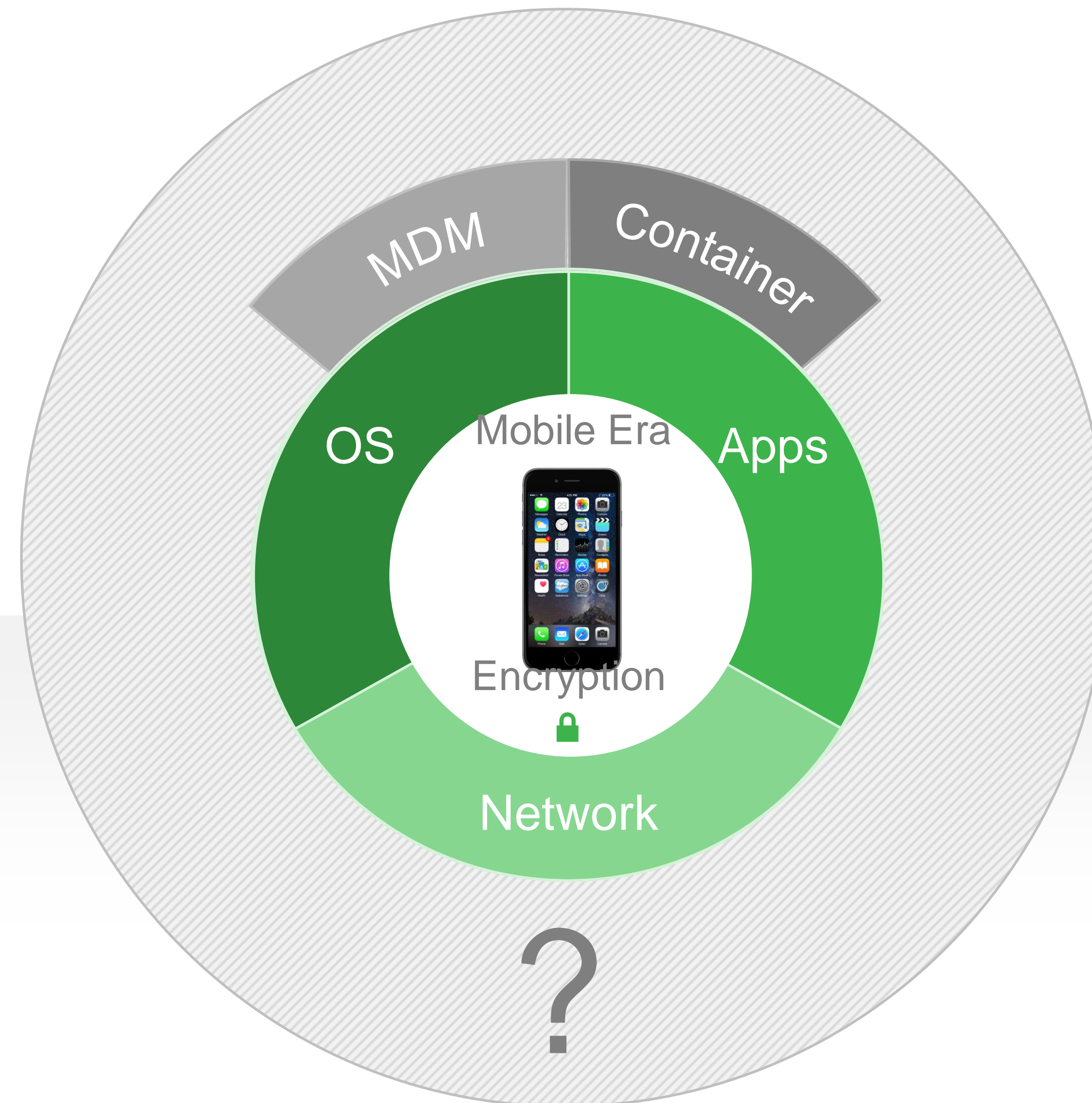
Personal data shall be....

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.



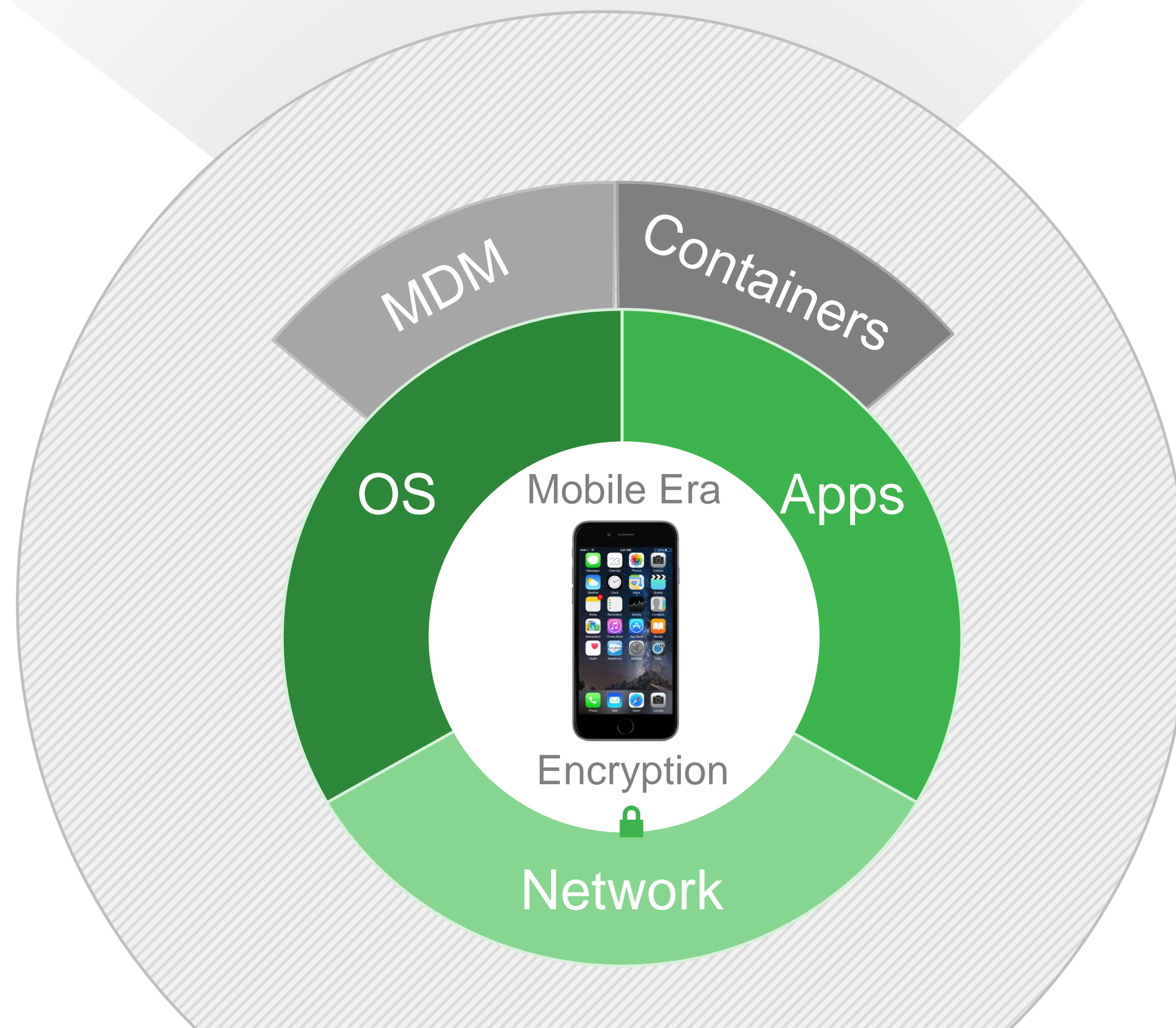
EMM + Security

vmware® airwatch®

Microsoft Intune

MobileIron

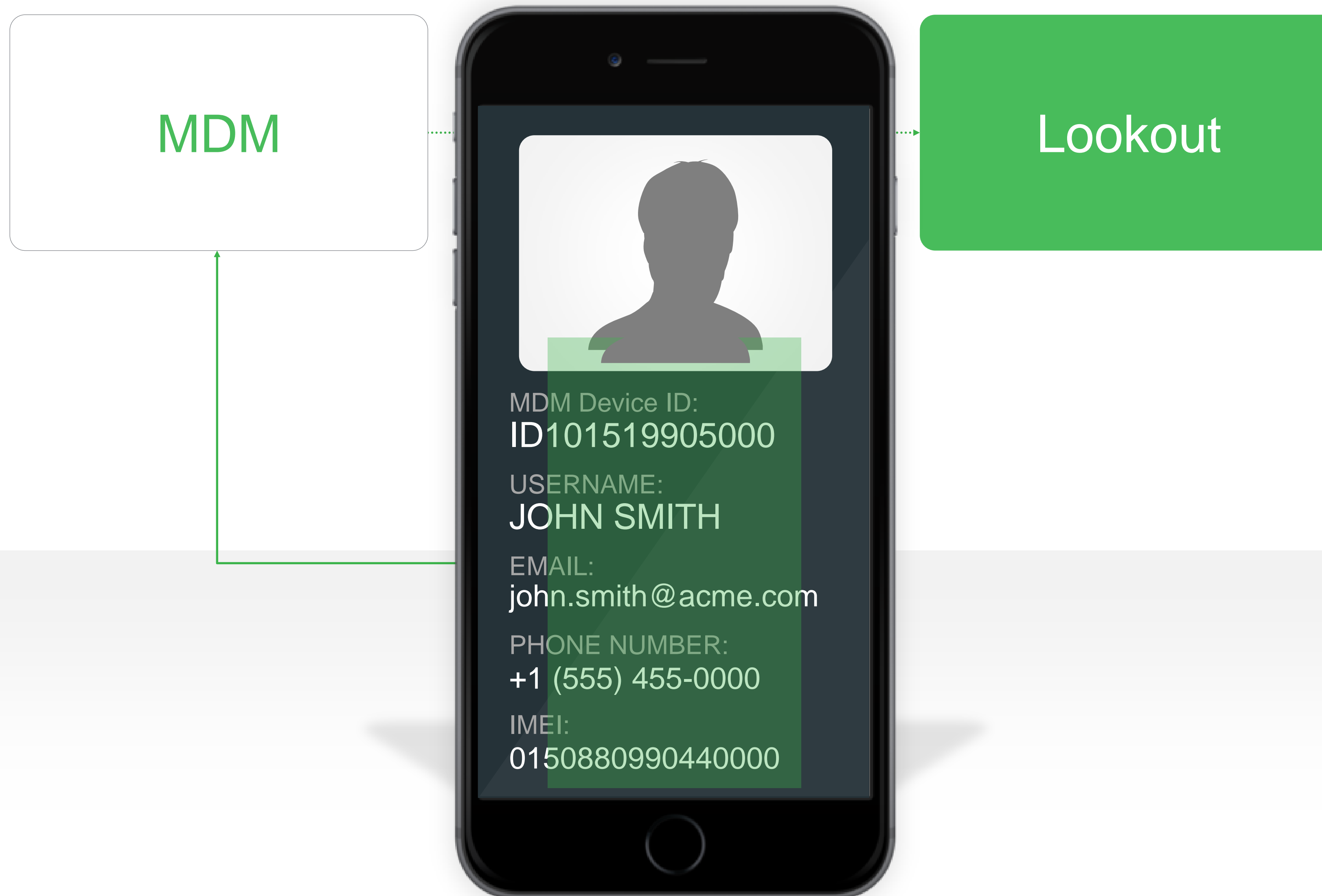
MaaS360®
by Fiberlink, an IBM company



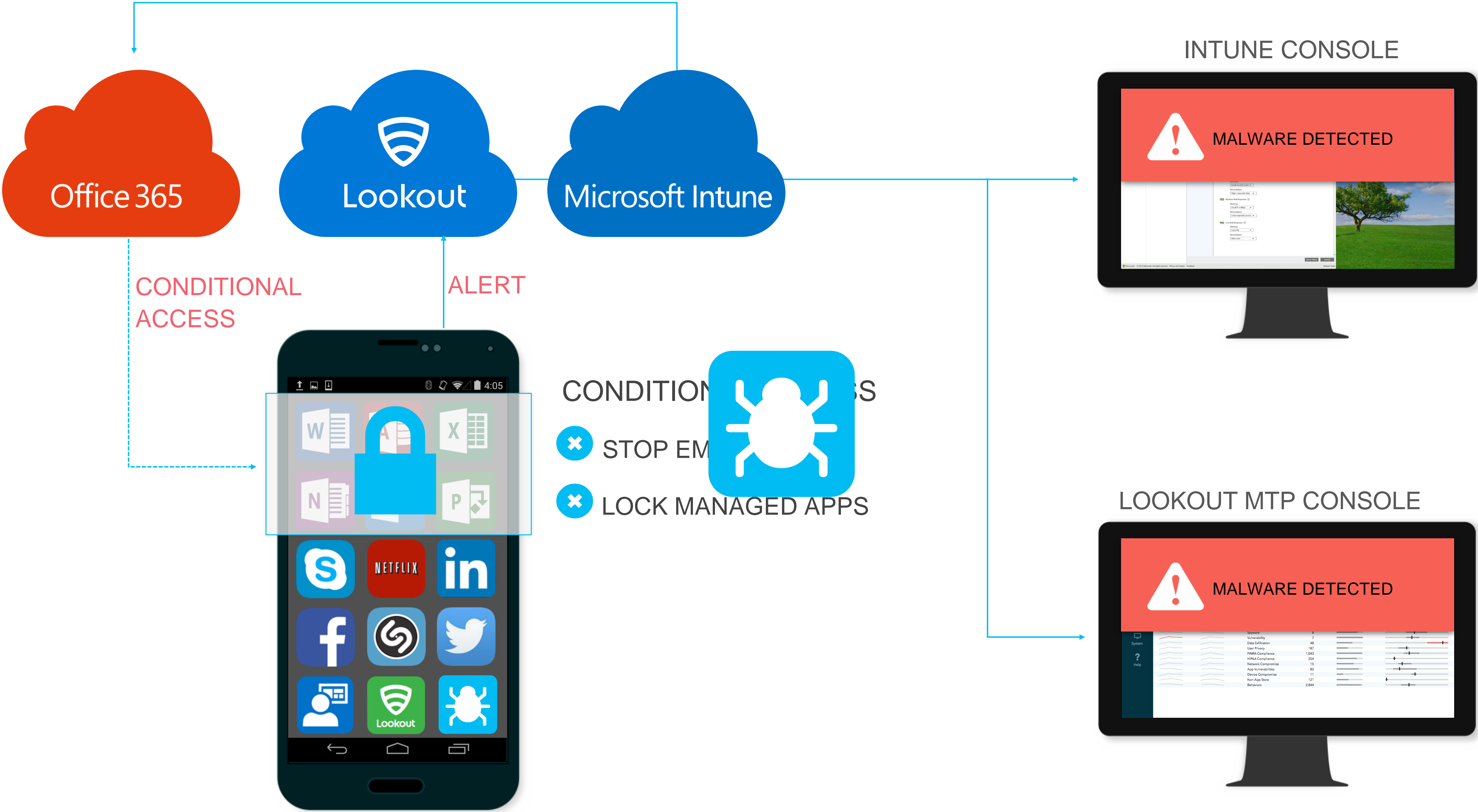
RISKS	EMM ONLY	SECURITY + EMM
Lost Device	✓ Protected	✓ Protected
App distribution	✓ Protected	✓ Protected
Policy violations	! Limited Protection	✓ Protected
Data leakage	! Limited Protection	✓ Protected
Jailbreaking & rooting	! Limited Protection	✓ Protected
Malicious apps	x No Protection	✓ Protected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

Privacy by design:

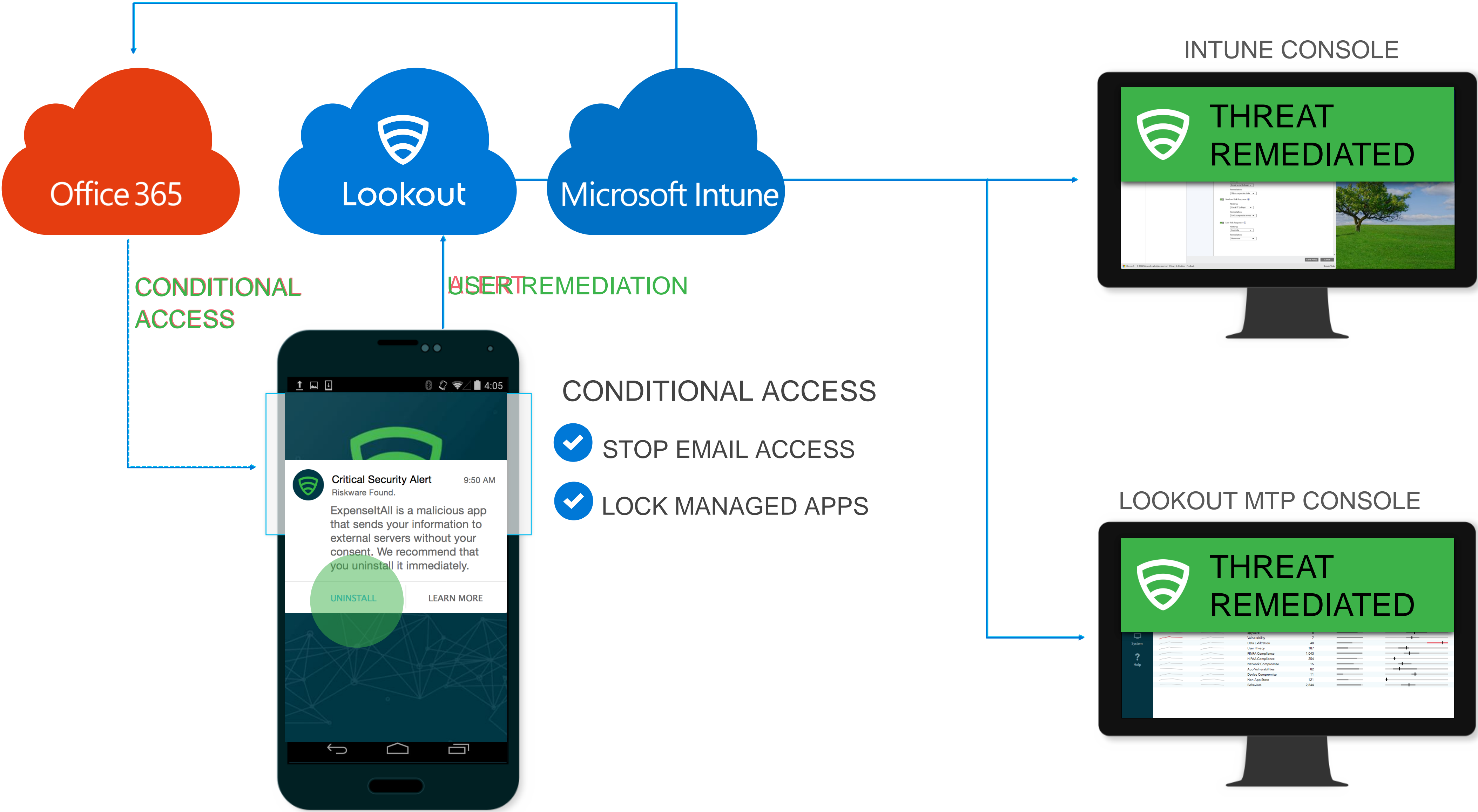
Data privacy controls limit what Lookout can see



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

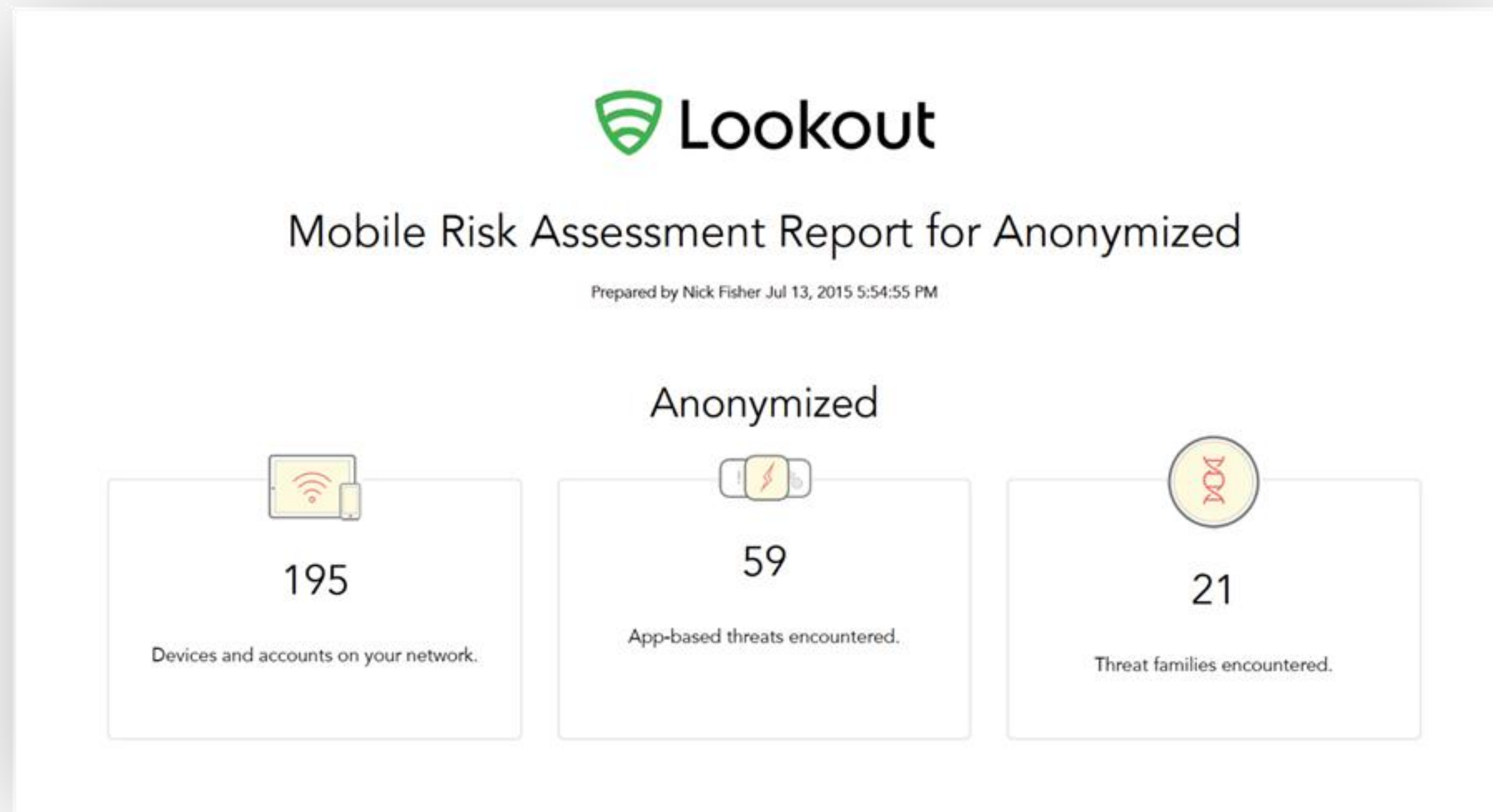
- 100% mobile threat remediation, completed by non-technical users
- Improved productivity for remote nurse teams
- Gained compliance with Dutch privacy laws regarding the security of private data on mobile devices
- Achieved visibility into network and app-based mobile threats with the potential to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

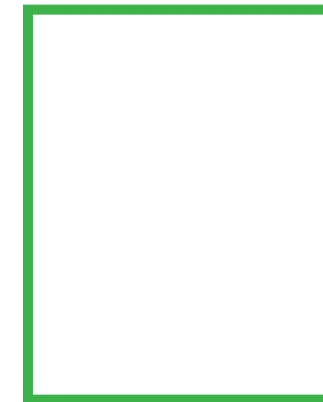
- Industry: Healthcare
- Device Policy: COPE
- MDM: MobileIron

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.





EVERYTHING WILL BE OK