The world has changed.

The data center is a cloud.

The corporate network is Starbucks WiFi.

Phones, tablets, and wearables have replaced managed laptops.

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

So what’s IT’s response to this change?

You restrict your users.

You manage devices.

Restrict background data?

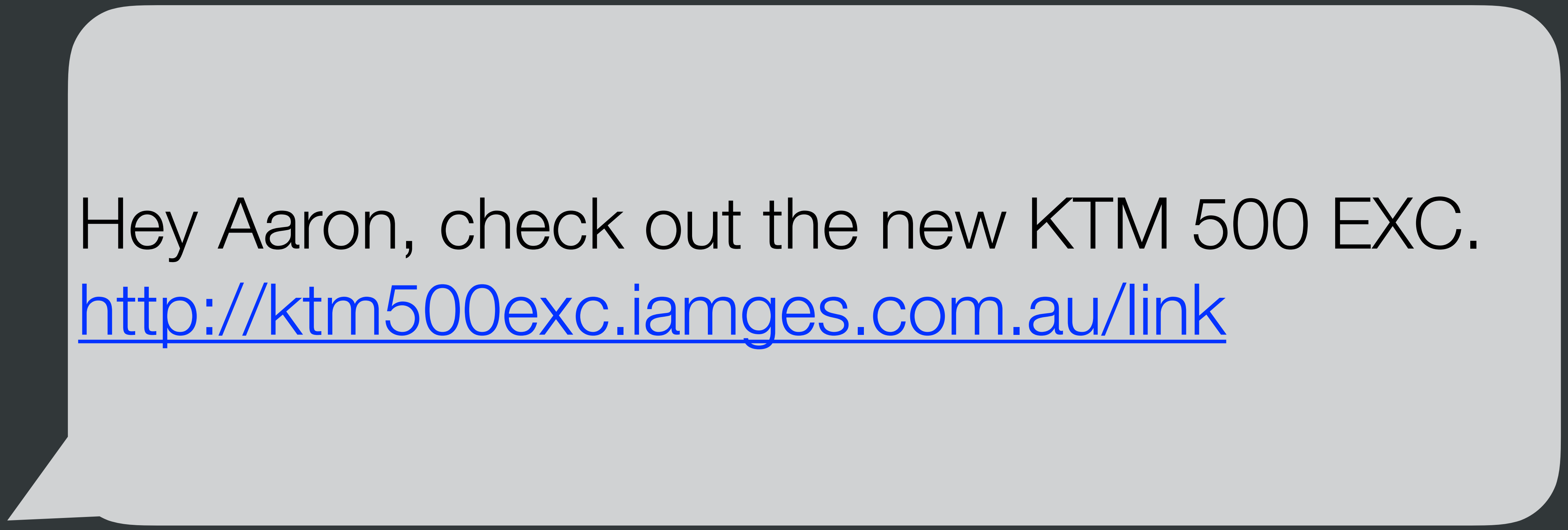
If you restrict background cellular data, some apps and services won't work unless you're connected to Wi-Fi.

This setting affects all users on this phone.

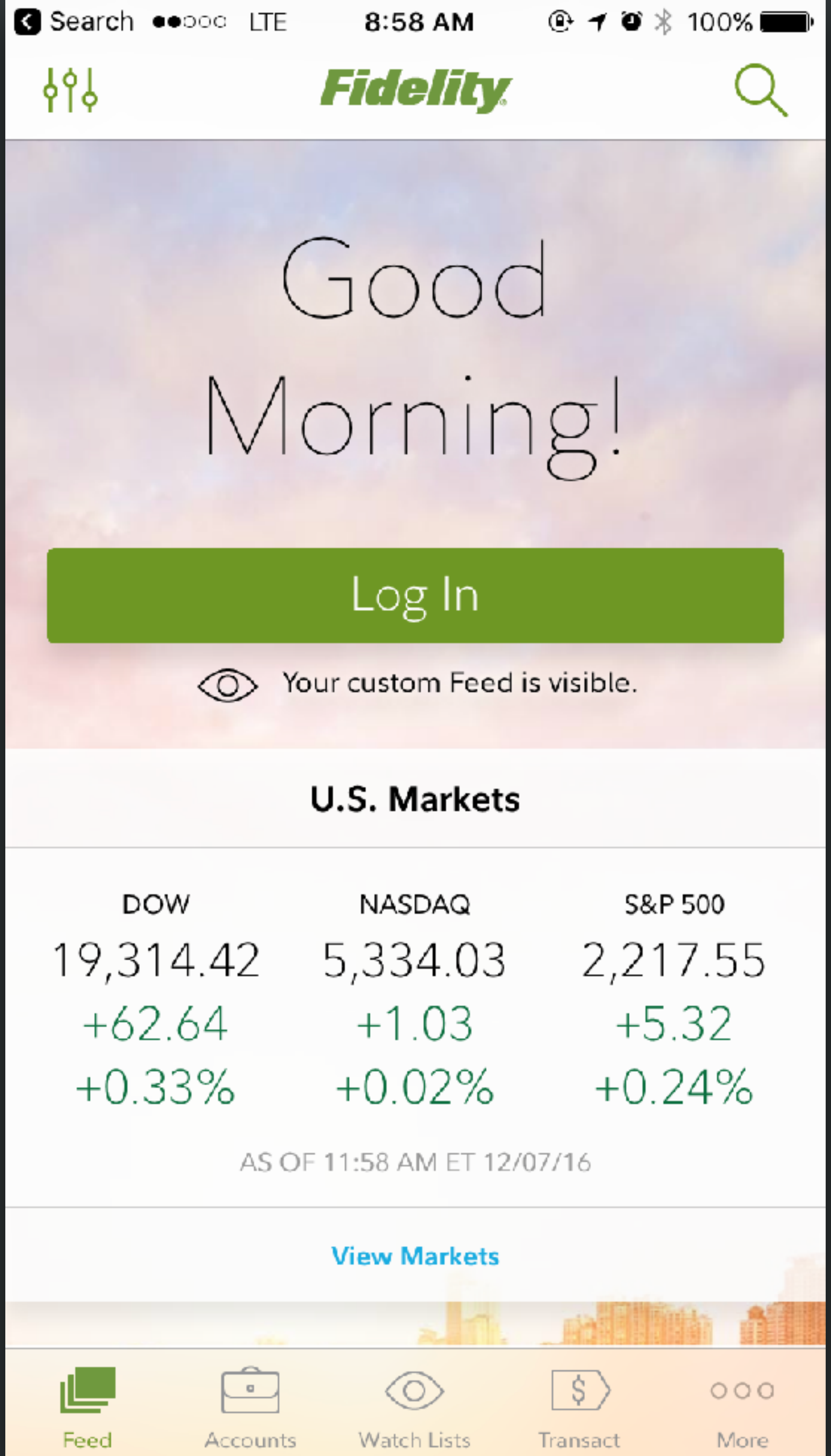
You lock down access.

…but mobile devices are personal.

…and because they’re personal, they’re the new target of attack.



Hey Aaron, check out the new KTM 500 EXC.
http://ktm500exc.iamges.com.au/link



Good Morning!

Log In

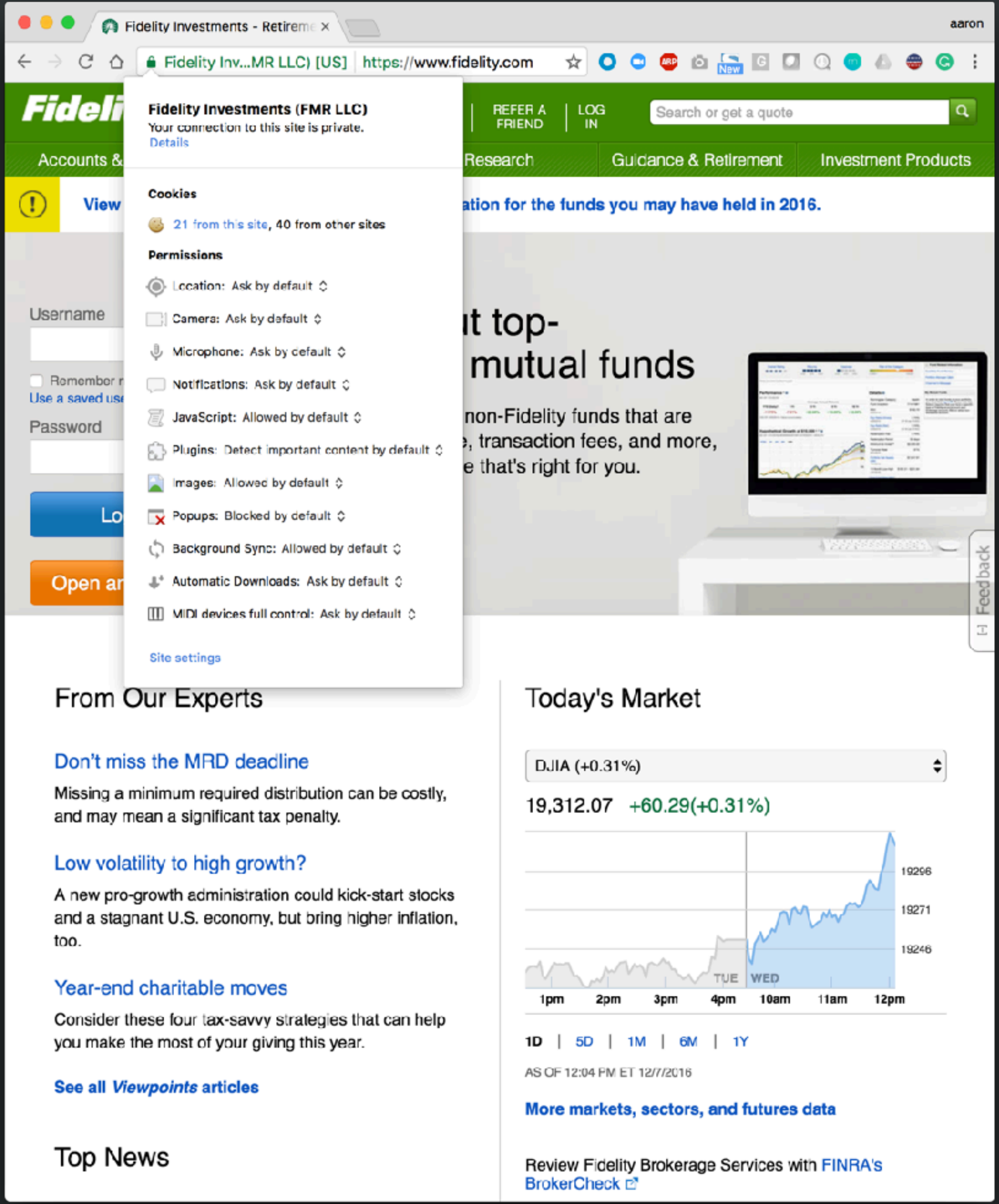
Your custom Feed is visible.

U.S. Markets

DOW	NASDAQ	S&P 500
19,314.42	5,334.03	2,217.55
+62.64	+1.03	+5.32
+0.33%	+0.02%	+0.24%

AS OF 11:58 AM ET 12/07/16

View Markets



Fidelity Investments (FMR LLC)
Your connection to this site is private.
Details

Cookies

21 from this site, 40 from other sites

Permissions

- Location: Ask by default
- Camera: Ask by default
- Microphone: Ask by default
- Notifications: Ask by default
- JavaScript: Allowed by default
- Plugins: Detect important content by default
- Images: Allowed by default
- Popups: Blocked by default
- Background Sync: Allowed by default
- Automatic Downloads: Ask by default
- MIDI devices full control: Ask by default

Site settings

View ation for the funds you may have held in 2016.

Username

Remember r
Use a saved use

Password

Lo

Open ar

t top-
mutual funds

non-Fidelity funds that are
, transaction fees, and more,
e that's right for you.

From Our Experts

Don't miss the MRD deadline

Missing a minimum required distribution can be costly, and may mean a significant tax penalty.

Low volatility to high growth?

A new pro-growth administration could kick-start stocks and a stagnant U.S. economy, but bring higher inflation, too.

Year-end charitable moves

Consider these four tax-savvy strategies that can help you make the most of your giving this year.

See all *Viewpoints* articles

Top News

Today's Market

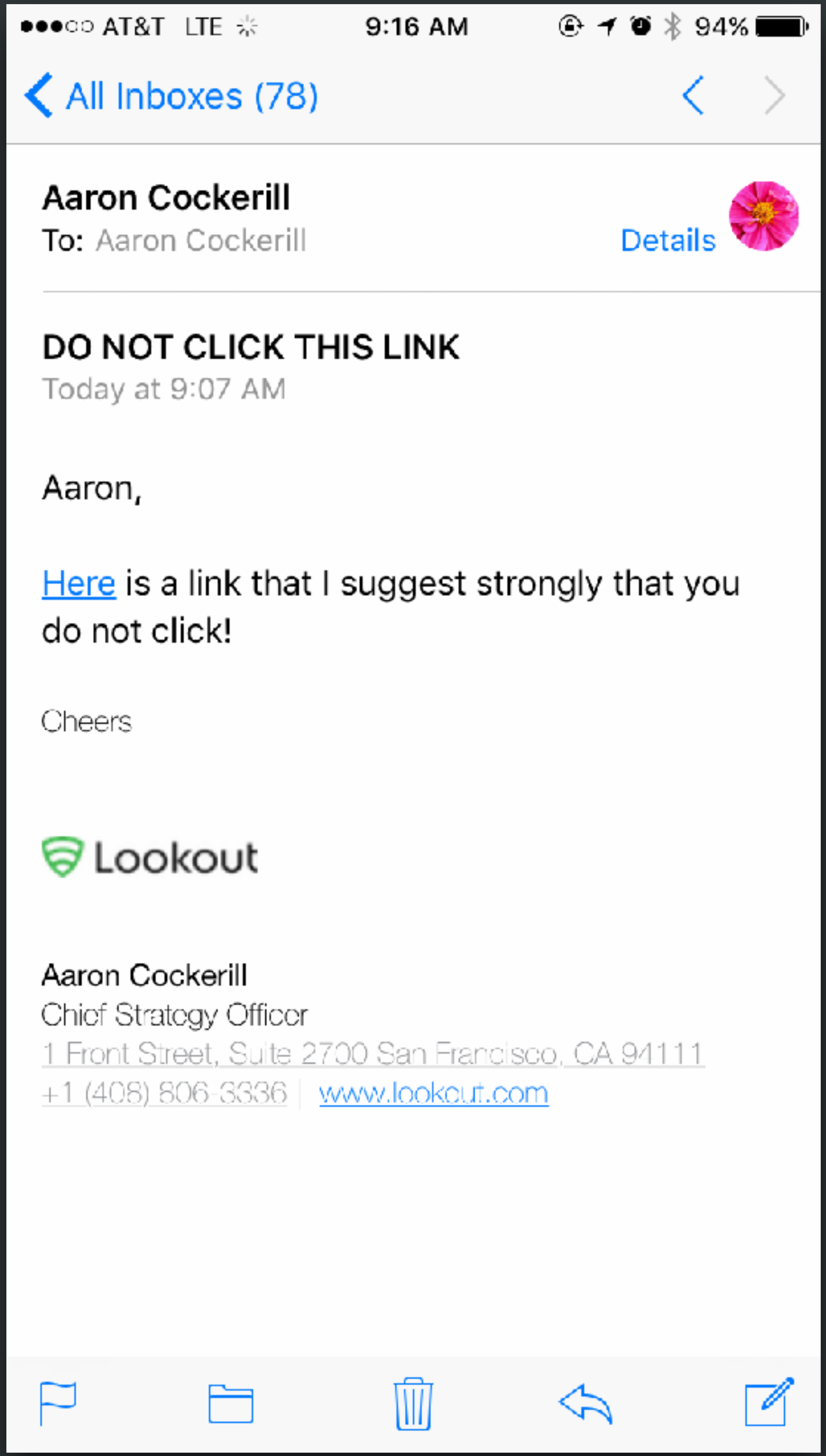
DJIA (+0.31%)

19,312.07 +60.29(+0.31%)

AS OF 12:04 PM ET 12/7/2016

More markets, sectors, and futures data

Review Fidelity Brokerage Services with FINRA's BrokerCheck



Aaron Cockerill
To: Aaron Cockerill

DO NOT CLICK THIS LINK
Today at 9:07 AM

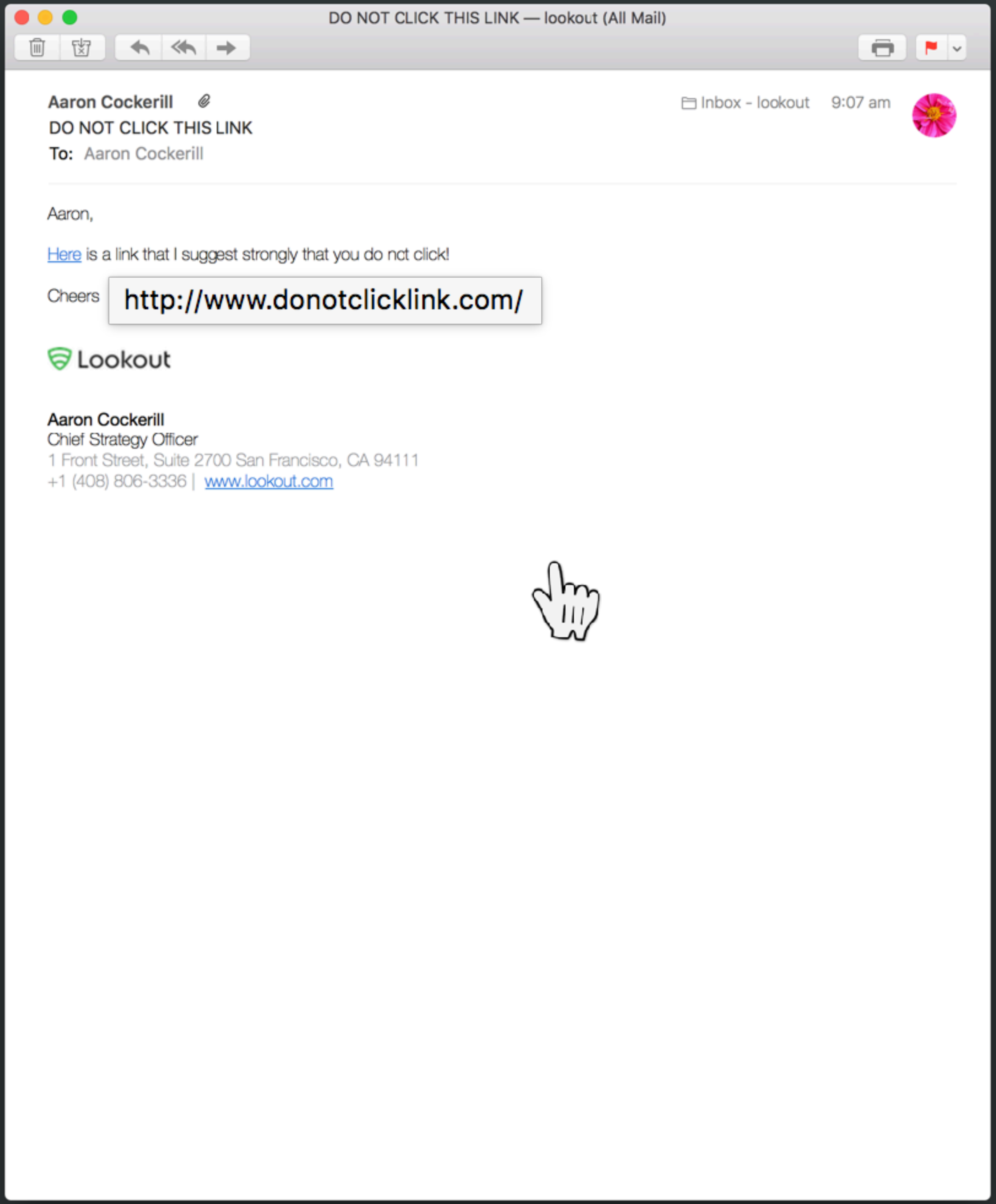
Aaron,

Here is a link that I suggest strongly that you do not click!

Cheers

Lookout

Aaron Cockerill
Chief Strategy Officer
1 Front Street, Suite 2700 San Francisco, CA 94111
+1 (408) 806-3336 | www.lookout.com



Aaron Cockerill
DO NOT CLICK THIS LINK
To: Aaron Cockerill

Aaron,

Here is a link that I suggest strongly that you do not click!

Cheers

http://www.donotclicklink.com/

Lookout

Aaron Cockerill
Chief Strategy Officer
1 Front Street, Suite 2700 San Francisco, CA 94111
+1 (408) 806-3336 | www.lookout.com

51%

Time on mobile, vs
42% on PC

KPCB | KLEINER PERKINS CAUFIELD BYERS

90%

Time in apps,
not the browser.

FLURRY

```
1010001 0100100 1001001 0010100
1001010 0100101 0100101 0010101
0100100 1010010 1010100 1010101
0100111 USER_ID PASSWRD 1010101
0010101 0101001 0010100 1001010
1010010 1011110 1010010 1010010
1010010 1010101 0101001 0101010
1001010 0101010 1010100 1010100
```

67%

Global 2000 companies
report breaches as a result
mobile devices

Ponemon Institute

Pegasus - a real life mobile exploit

TRUMP: *The* YEAR *of* LIVING SHORT-FINGEREDLY / *By* GRAYDON CARTER

INSIDE the KARDASHIAN PARIS HOTEL HEIST! / *By* MARK SEAL

VANITY FAIR

HOLIDAY 2016/2017

ALSO

WHAT DOES PETER THIEL REALLY WANT? *By* DAVID MARGOLICK

AIRBNB 2.0: HALFWAY TO WESTWORLD? *By* KATRINA BROOKER

The 2016 *Holiday* GIFT GUIDE

BIGGER! BETTER! NO NUTCRACKERS!

PLUS

WHO HACKED SILICON VALLEY'S CROWN JEWEL? *By* BRYAN BURROUGH

Baby, It's Hot Outside

J. Law!

IF THERE'S ONE PERSON WHO CAN REDEEM 2016, IT'S THE FREEWHEELIN' JENNIFER LAWRENCE

By JULIE MILLER *Photographs by* PETER LINDBERGH

"OH, MUST WE DREAM OUR DREAMS AND HAVE THEM, TOO?" —*Elizabeth Bishop*

The Making of *A Christmas Story* *By* SAM KASHNER

The Dark, Nasty Side of ... Maple Syrup?! *By* RICH COHEN

INVADING APPLE

What if a government could wirelessly control any iPhone? Last summer, a University of California grad student named Bill Marczak stumbled across a piece of spyware that would do just that. Probing a new arena of cyber-warfare, in which shadowy firms sell spyware to repressive regimes such as those in Bahrain, Egypt, and Uganda, BRYAN BURROUGH reveals the details of the hack that shocked Apple and security experts worldwide

Top: Max Bazaliy. Right: Mike Murray, Andrew Blaich, Kristy Edwards, Seth Hardy

Th in.

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objective

Reconnaissance

Weaponization

Delivery

Exploitation

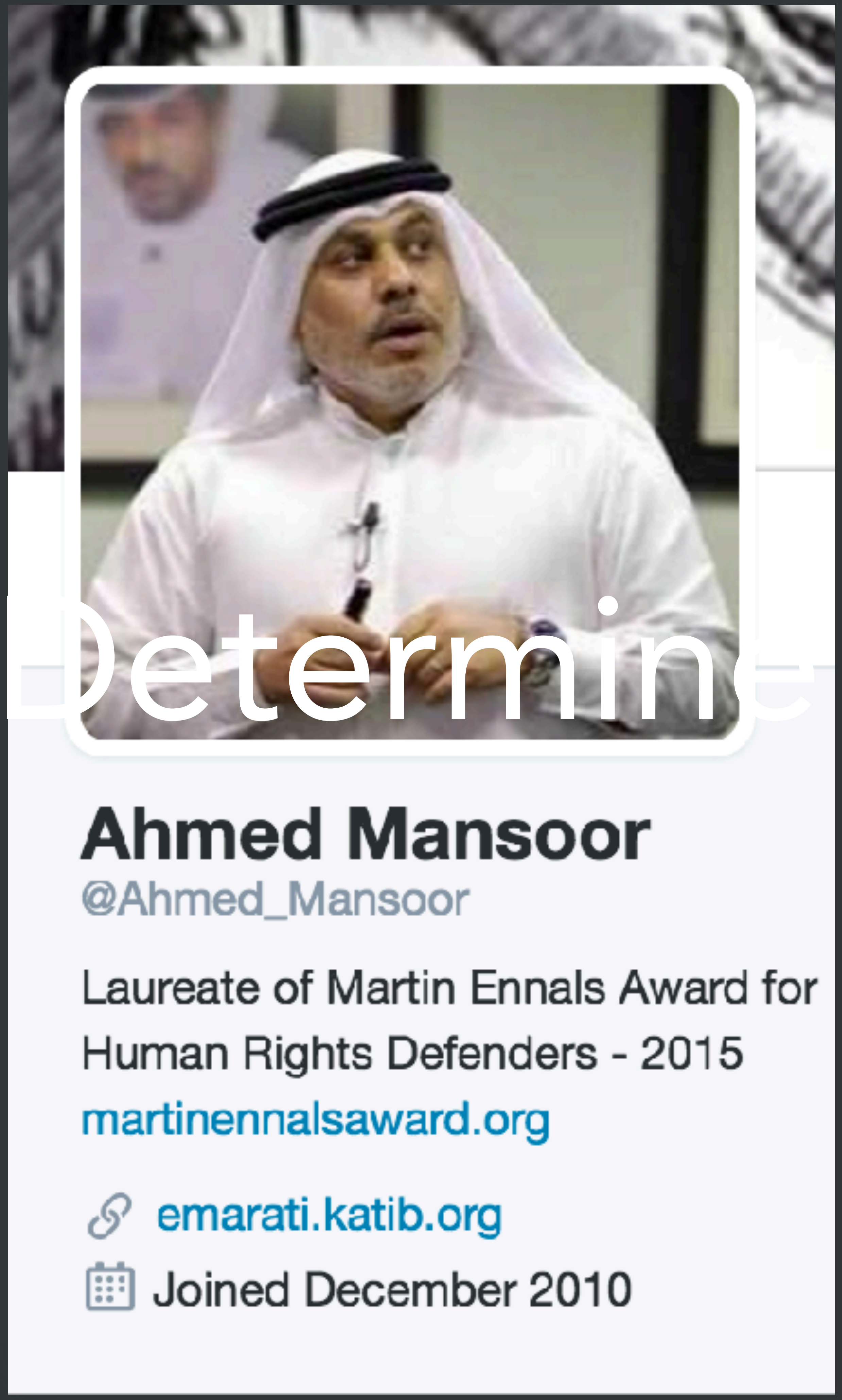
Installation

Command & Control

Actions on Objective

Determine ta

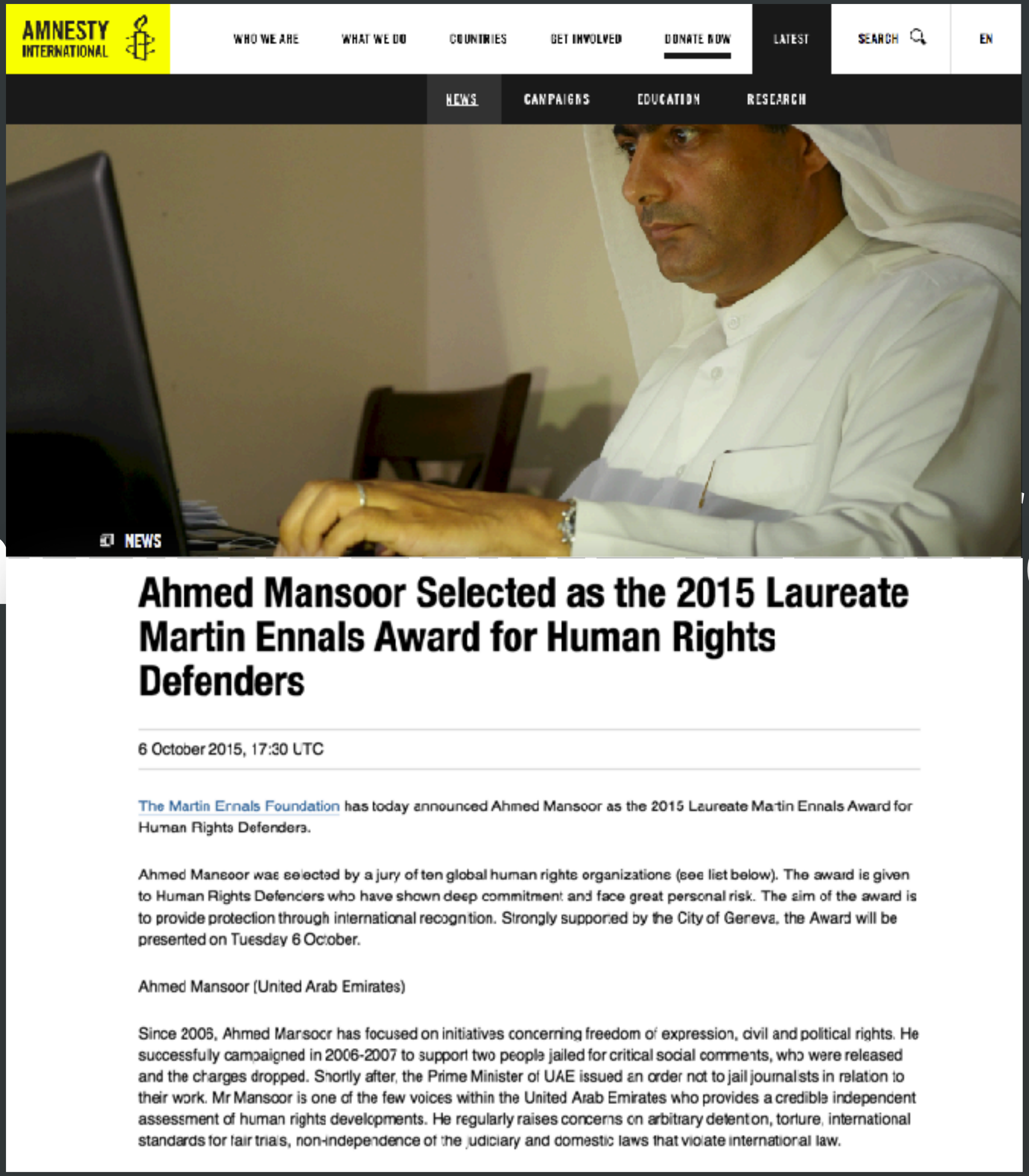
o



Ahmed Mansoor
@Ahmed_Mansoor

Laureate of Martin Ennals Award for Human Rights Defenders - 2015
martinennalsaward.org

emarati.katib.org
Joined December 2010



Ahmed Mansoor Selected as the 2015 Laureate Martin Ennals Award for Human Rights Defenders

6 October 2015, 17:30 UTC

The Martin Ennals Foundation has today announced Ahmed Mansoor as the 2015 Laureate Martin Ennals Award for Human Rights Defenders.

Ahmed Mansoor was selected by a jury of ten global human rights organizations (see list below). The award is given to Human Rights Defenders who have shown deep commitment and face great personal risk. The aim of the award is to provide protection through international recognition. Strongly supported by the City of Geneva, the Award will be presented on Tuesday 6 October.

Ahmed Mansoor (United Arab Emirates)

Since 2005, Ahmed Mansoor has focused on initiatives concerning freedom of expression, civil and political rights. He successfully campaigned in 2006-2007 to support two people jailed for critical social comments, who were released and the charges dropped. Shortly after, the Prime Minister of UAE issued an order not to jail journalists in relation to their work. Mr Mansoor is one of the few voices within the United Arab Emirates who provides a credible independent assessment of human rights developments. He regularly raises concerns on arbitrary detention, torture, international standards for fair trials, non-independence of the judiciary and domestic laws that violate international law.

- Reconnaissance
- **Weaponization**
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objective

Package initi

ccess exploit

Reconnaissance

Weaponization

Delivery

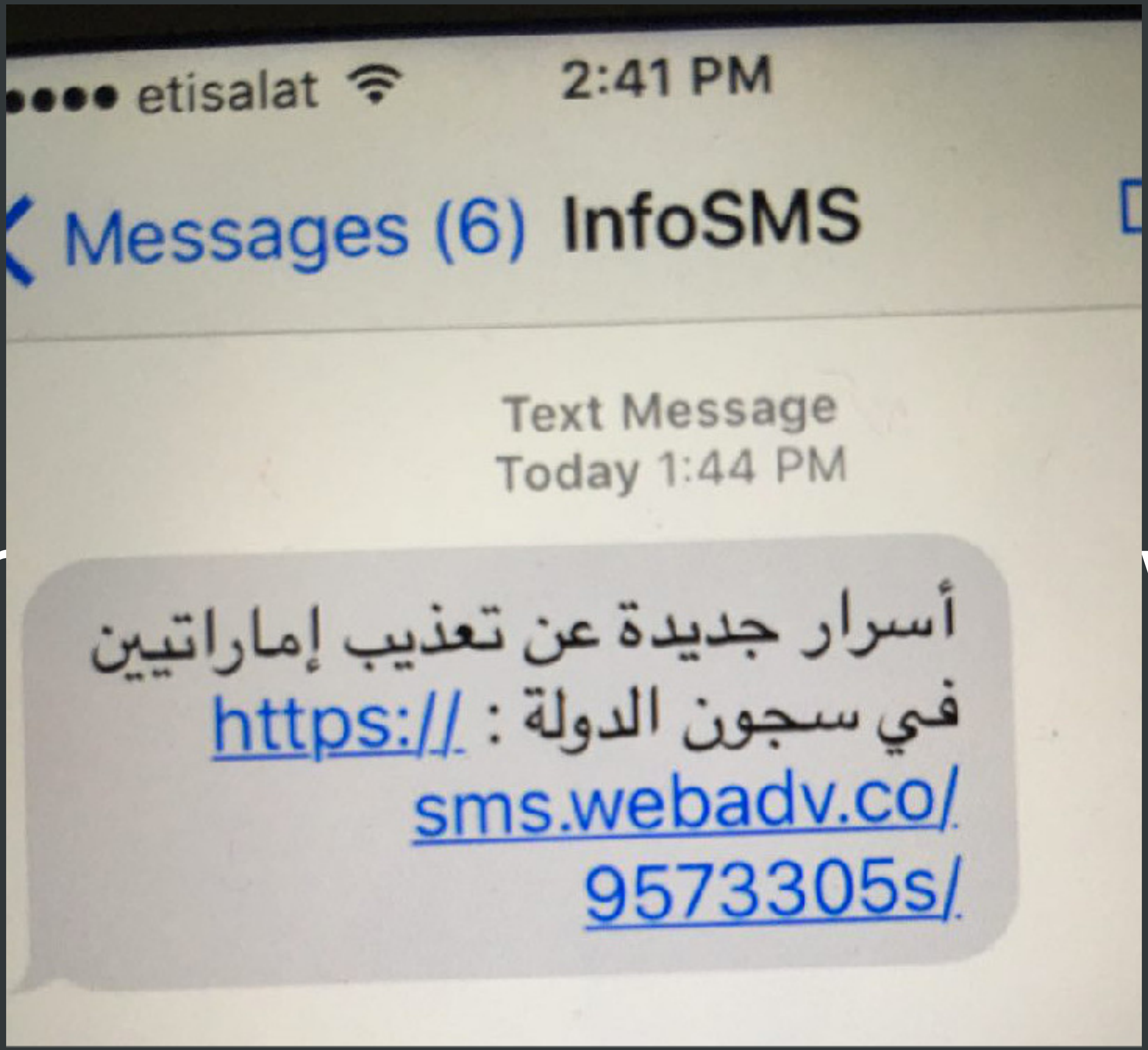
Exploitation

Installation

Command & Control

Actions on Objective

Socially er

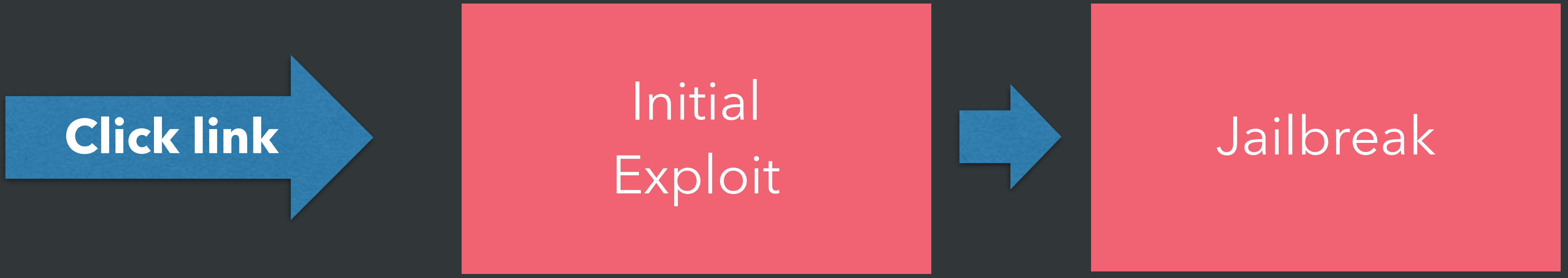


Text Message
Today 1:44 PM

أسرار جديدة عن تعذيب إماراتيين
في سجون الدولة : https://
sms.webadv.co/
9573305s/

web page

- Reconnaissance
- Weaponization
- Delivery
- **Exploitation**
- Installation
- Command & Control
- Actions on Objective



Exploit against Safari

- CVE-2016-4655

3 zero days

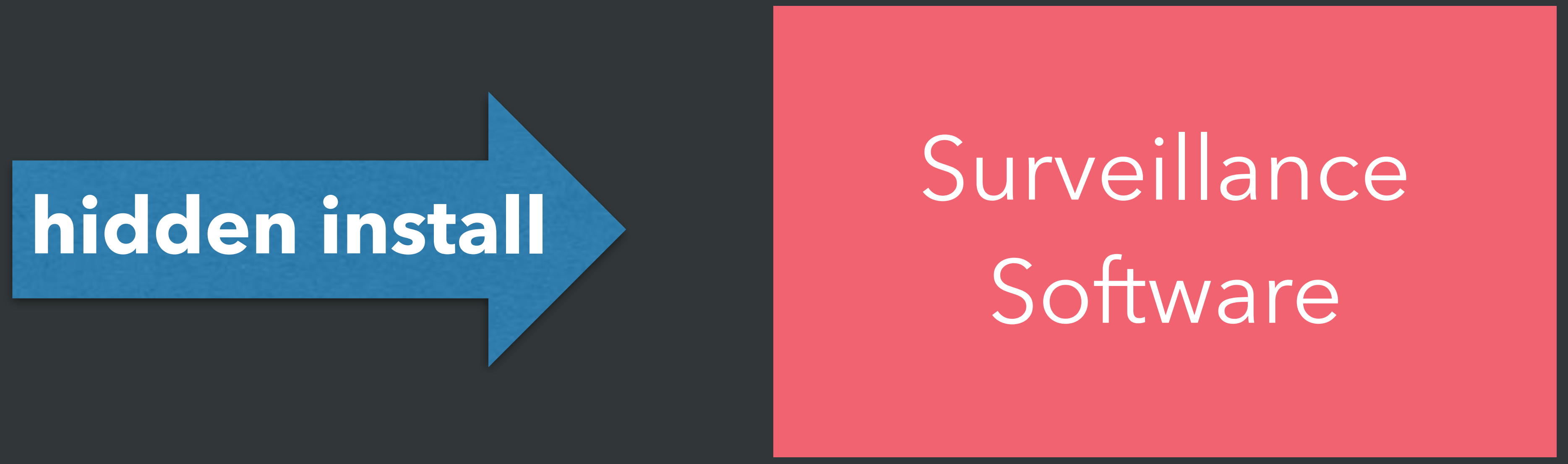
Two kernel exploits:

- CVE-2016-4656
- CVE-2016-4657

jailbreak the device

Multi-stage iOS exploit

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- **Installation**
- Command & Control
- Actions on Objective



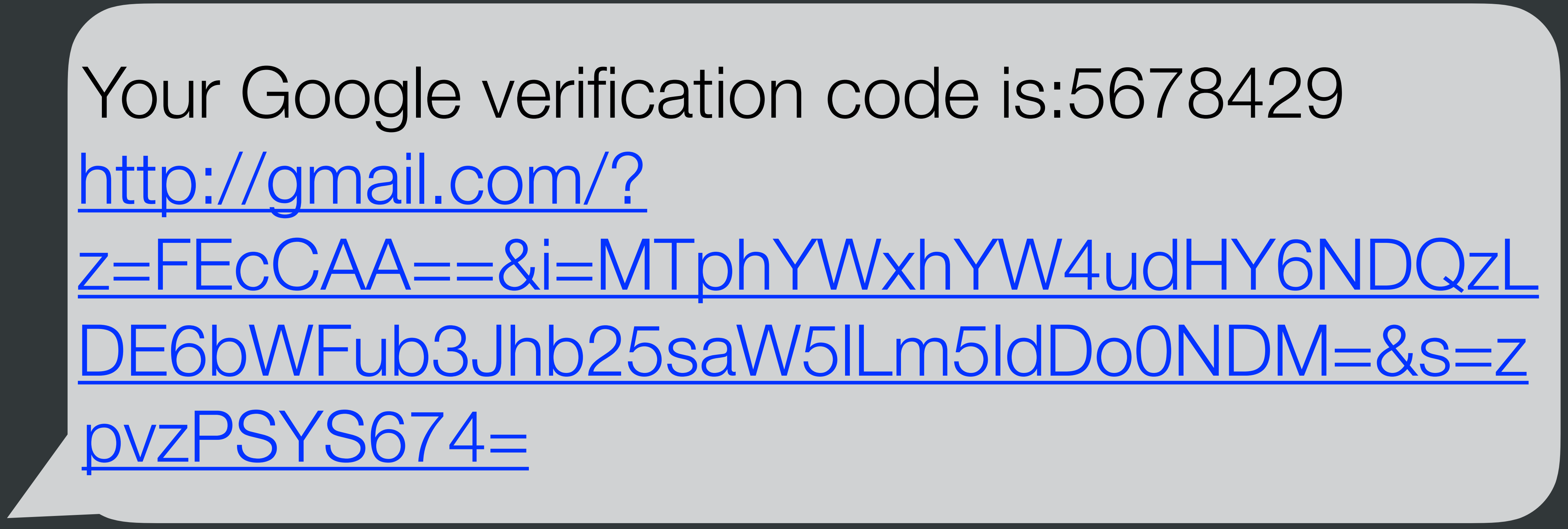
- Installs persistent stealth monitoring
- Establishes communication to Command & Control infrastructure
- Hooks all communication and starts stealing data

Sophisticated Capabilities

- Auto-start on reboot
- Re-exploit the kernel to maintain root privileges
- Disable iOS firmware updates
- Self-destruct if phone is tampered with

Installs persistent malware implant

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- **Command & Control**
- Actions on Objective



Your Google verification code is:5678429
http://gmail.com/?
z=FEcCAA==&i=MTphYWxhYW4udHY6NDQzL
DE6bWFub3Jhb25saW5lLm5ldDo0NDM=&s=z
pvzPSYS674=

Remotely control device

Reconnaissance

Weaponization

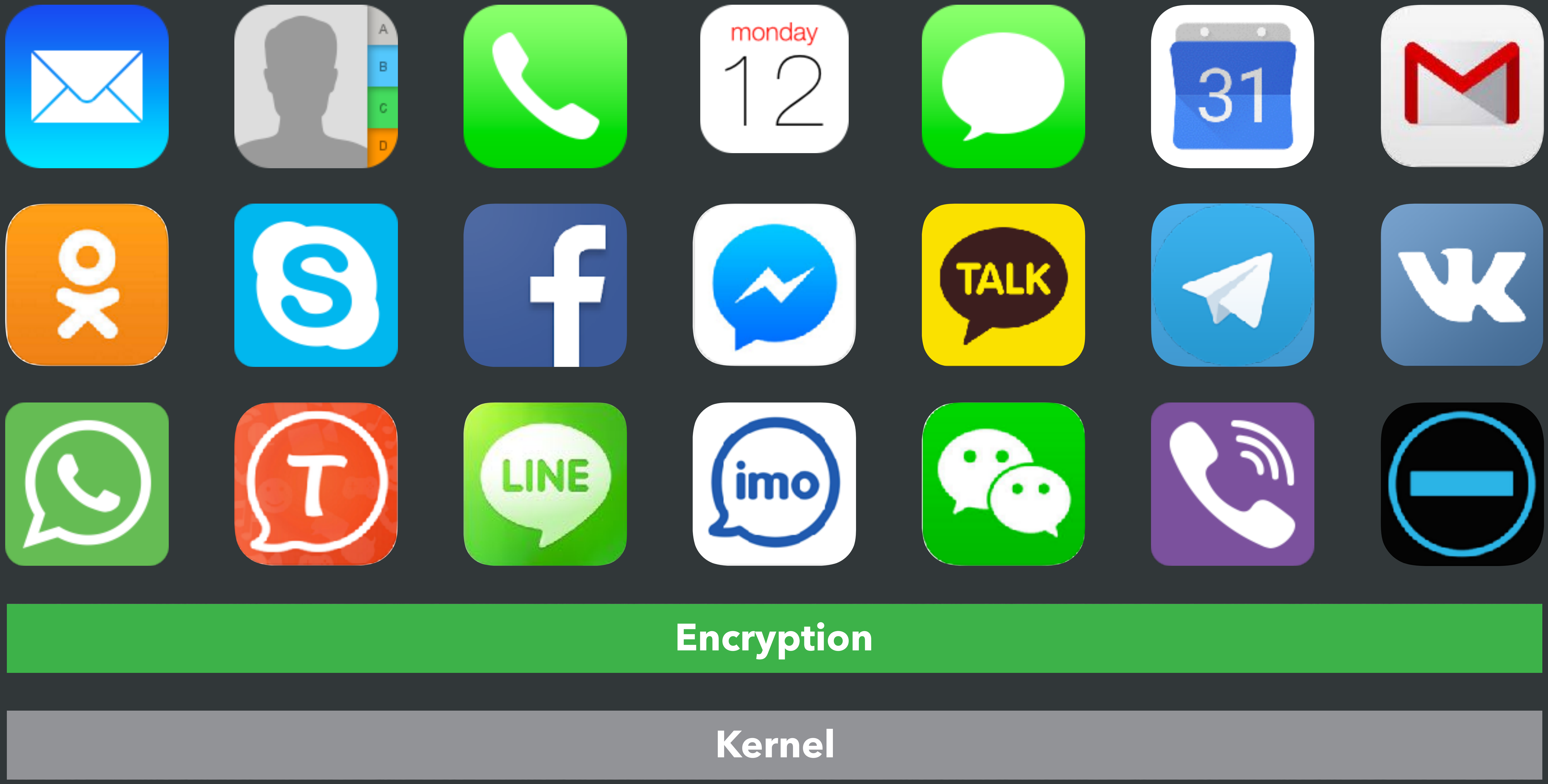
Delivery

Exploitation

Installation

Command & Control

Actions on Objective

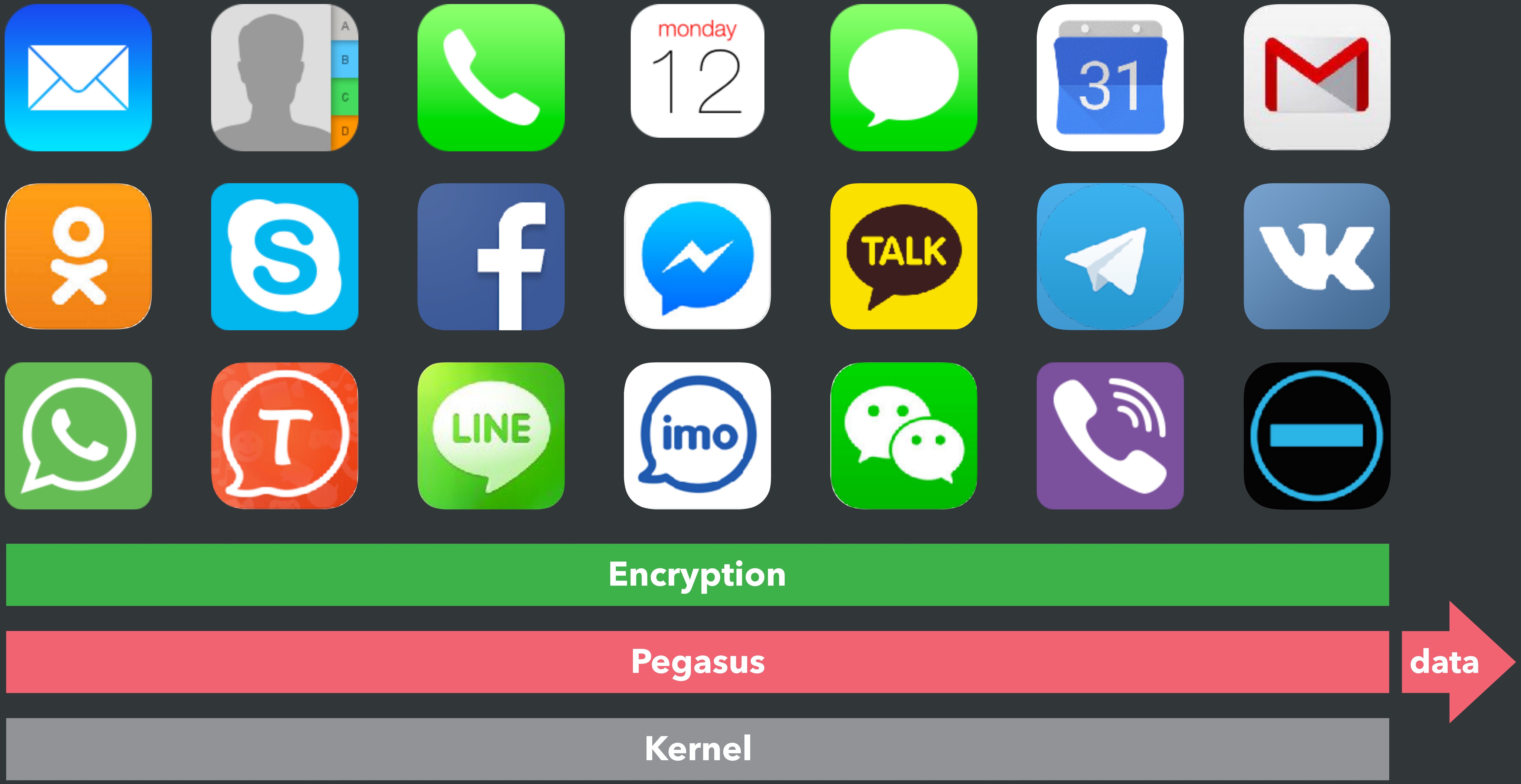


Encryption

Kernel

Exfiltrate data

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- **Actions on Objective**



Encryption

Pegasus

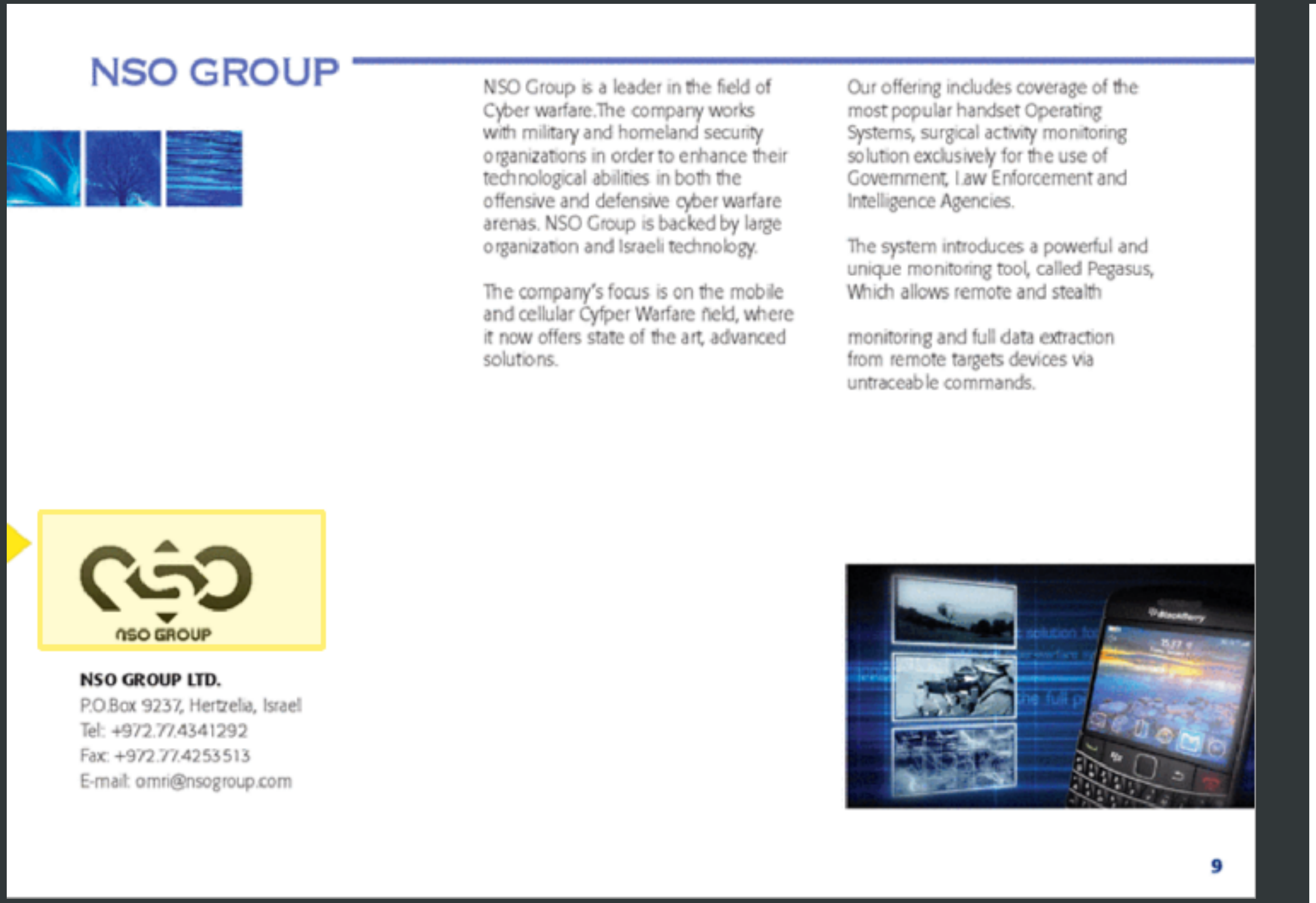
data

Kernel

Exfiltrate data

The Arms Dealer: NSO Group

"NSO Group is a leader in the field of Cyber warfare."


NSO GROUP

NSO Group is a leader in the field of Cyber warfare.The company works with military and homeland security organizations in order to enhance their technological abilities in both the offensive and defensive cyber warfare arenas. NSO Group is backed by large organization and Israeli technology.

The company's focus is on the mobile and cellular Cyfper Warfare field, where it now offers state of the art, advanced solutions.

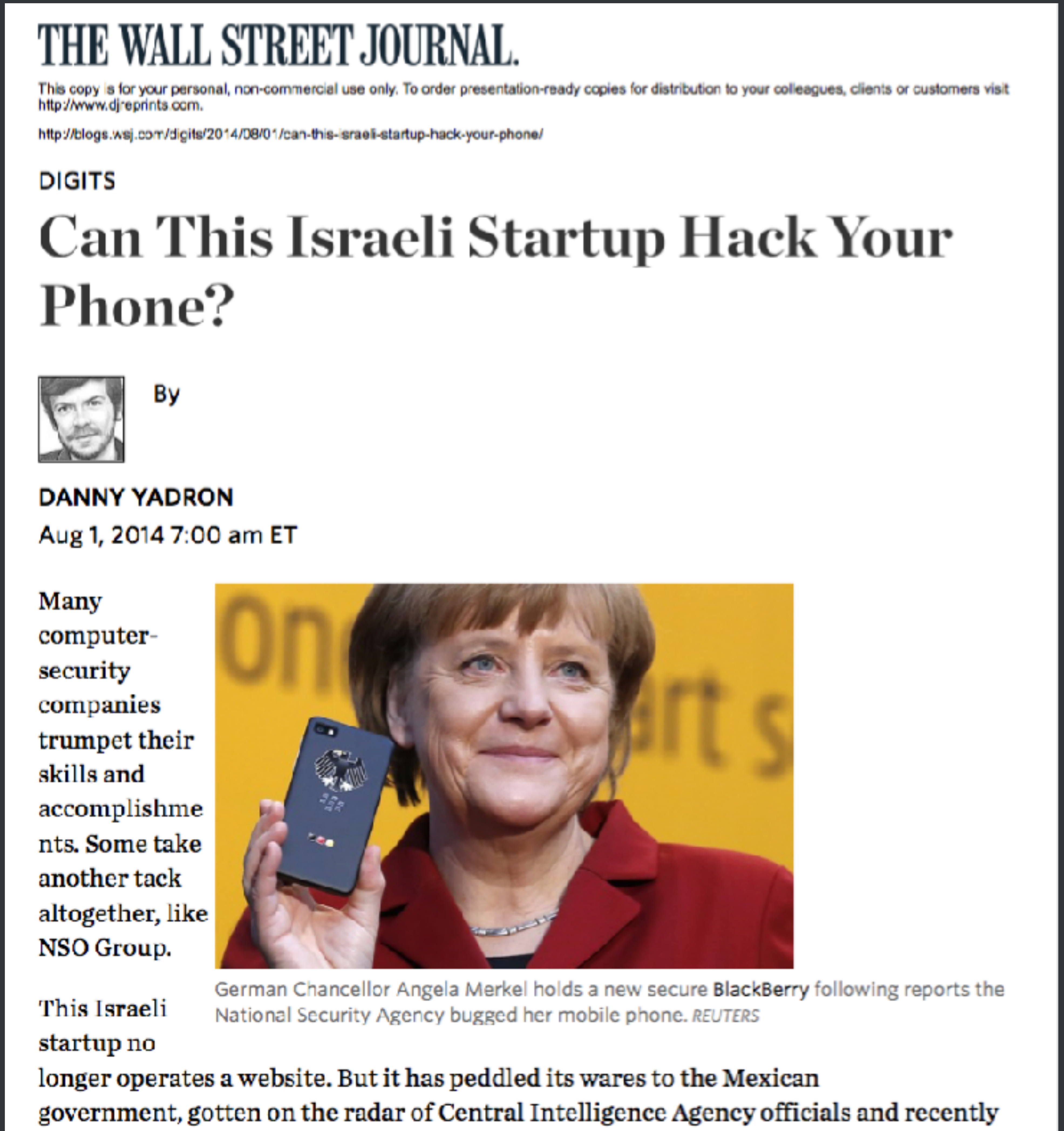
Our offering includes coverage of the most popular handset Operating Systems, surgical activity monitoring solution exclusively for the use of Government, Law Enforcement and Intelligence Agencies.

The system introduces a powerful and unique monitoring tool, called Pegasus, Which allows remote and stealth

monitoring and full data extraction from remote targets devices via untraceable commands.

NSO GROUP LTD.
P.O.Box 9237, Hertzelia, Israel
Tel: +972.77.4341292
Fax: +972.77.4253513
E-mail: omri@nsogroup.com

9


THE WALL STREET JOURNAL.

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit http://www.djreprints.com.

http://blogs.wsj.com/digits/2014/08/01/can-this-israeli-startup-hack-your-phone/

DIGITS

Can This Israeli Startup Hack Your Phone?

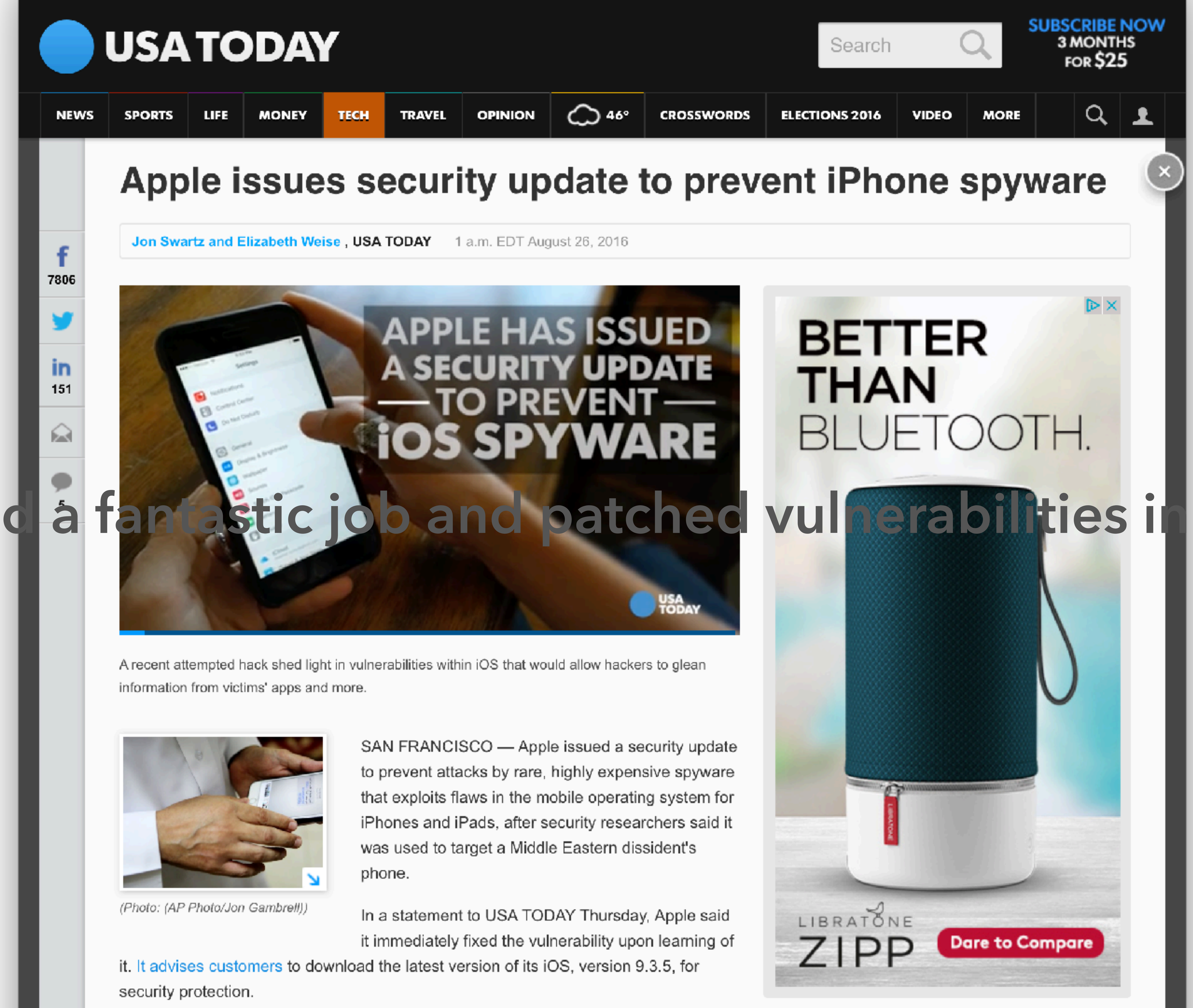
By

DANNY YADRON
Aug 1, 2014 7:00 am ET

Many computer-security companies trumpet their skills and accomplishments. Some take another tack altogether, like NSO Group.

German Chancellor Angela Merkel holds a new secure BlackBerry following reports the National Security Agency bugged her mobile phone. *REUTERS*

This Israeli startup no longer operates a website. But it has peddled its wares to the Mexican government, gotten on the radar of Central Intelligence Agency officials and recently



Apple issues security update to prevent iPhone spyware

Jon Swartz and Elizabeth Weise , USA TODAY 1 a.m. EDT August 26, 2016

A recent attempted hack shed light in vulnerabilities within iOS that would allow hackers to glean information from victims' apps and more.

(Photo: (AP Photo/Jon Gambrell))

SAN FRANCISCO — Apple issued a security update to prevent attacks by rare, highly expensive spyware that exploits flaws in the mobile operating system for iPhones and iPads, after security researchers said it was used to target a Middle Eastern dissident's phone.

In a statement to USA TODAY Thursday, Apple said it immediately fixed the vulnerability upon learning of it. It advises customers to download the latest version of its iOS, version 9.3.5, for security protection.

Apple did a fantastic job and patched vulnerabilities in 10 days!

What did your organization do?

Confiscate and replace 600 exec devices

+
−
Colorado Ave
Berkeley St
Stanford St
Franklin St
A St
A St
Stewart St
Nebraska Ave
Olympic Blvd
iPhone
12 minutes ago
□ Notify me when found
y Sound
Lost Mode
Erase iPhone
Cancel
Erase
Legal
Standard

Erase this iPhone?

All your content and settings will be erased when this iPhone connects to the Internet. An erased iPhone cannot be located or tracked.

Wipe all 1,500 un-patched devices

Gartner Predicts 2017

Key findings

- “Mobile attacks (Pegasus, XcodeGhost) and vulnerabilities (Stagefright, Heartbleed) are increasing in terms of both number and pragmatism.”
- “Enterprises are now looking for solutions that can enhance their mobile security posture.”

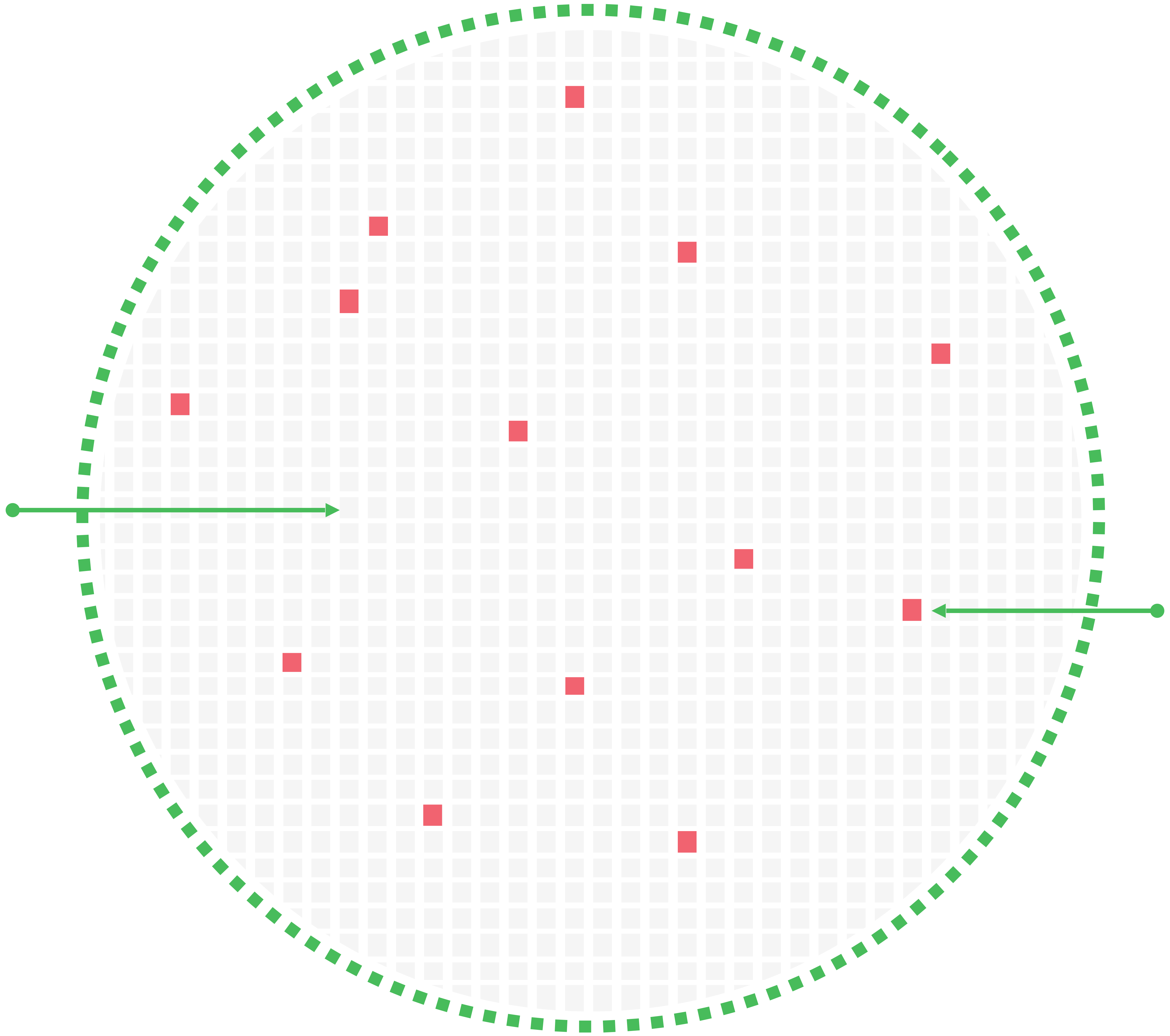
Security and risk managers responsible for endpoint and mobile security must

“Start now to evaluate MTD tools, and gradually implement these solutions in complement to EMM. ”

Source: Gartner Predicts 2017: Endpoint and Mobile Security, John Girard, Dionisio Zumerle, Brian Reed, Peter Firstbrook, Bart Willemsen, November 2016

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

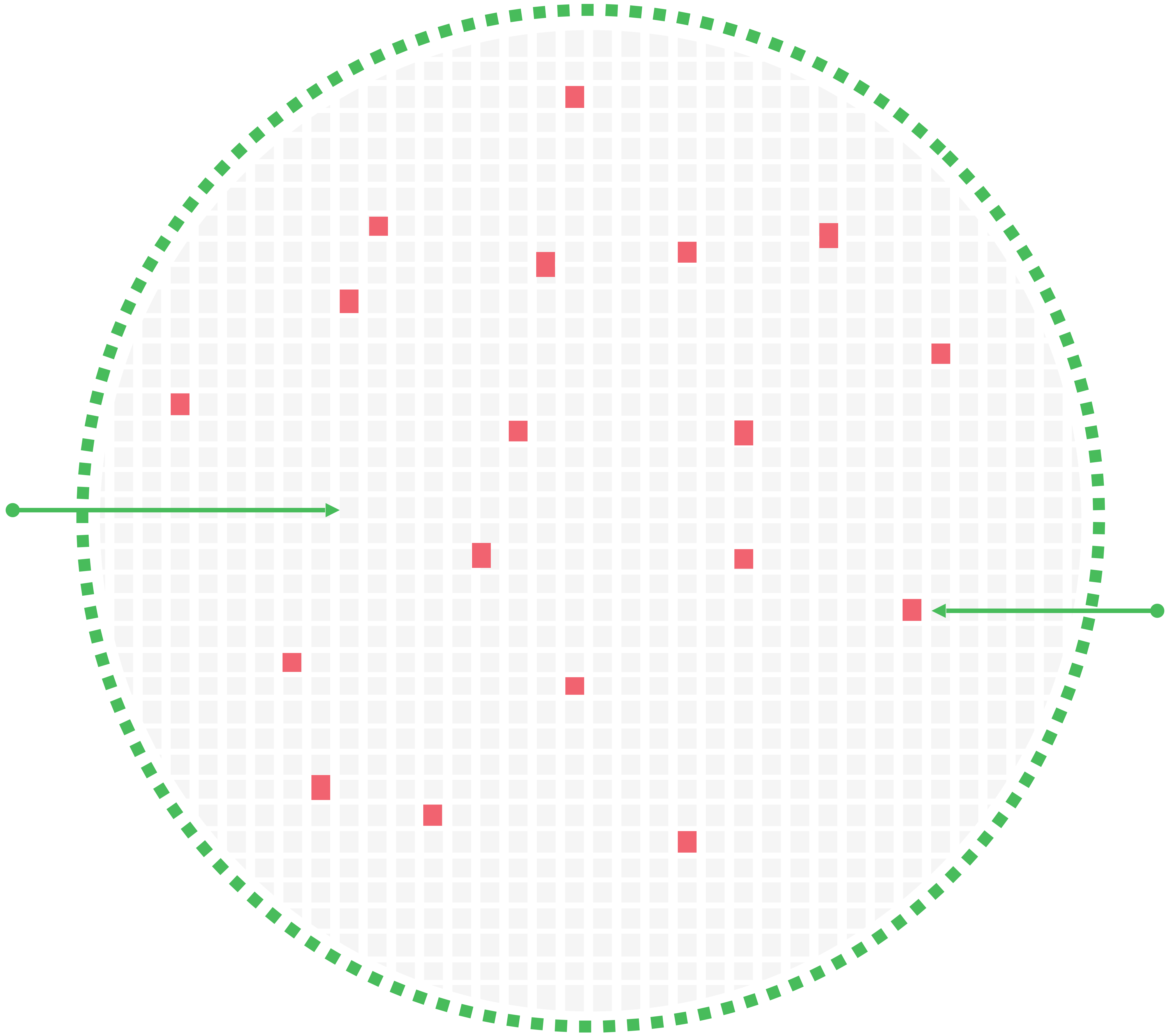
General threat encounter rate for enterprise mobile devices



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

…nearly **30** encountered serious threats

Threat encounter rate for **Retail Sector** mobile devices



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

… **45** serious threats, of which

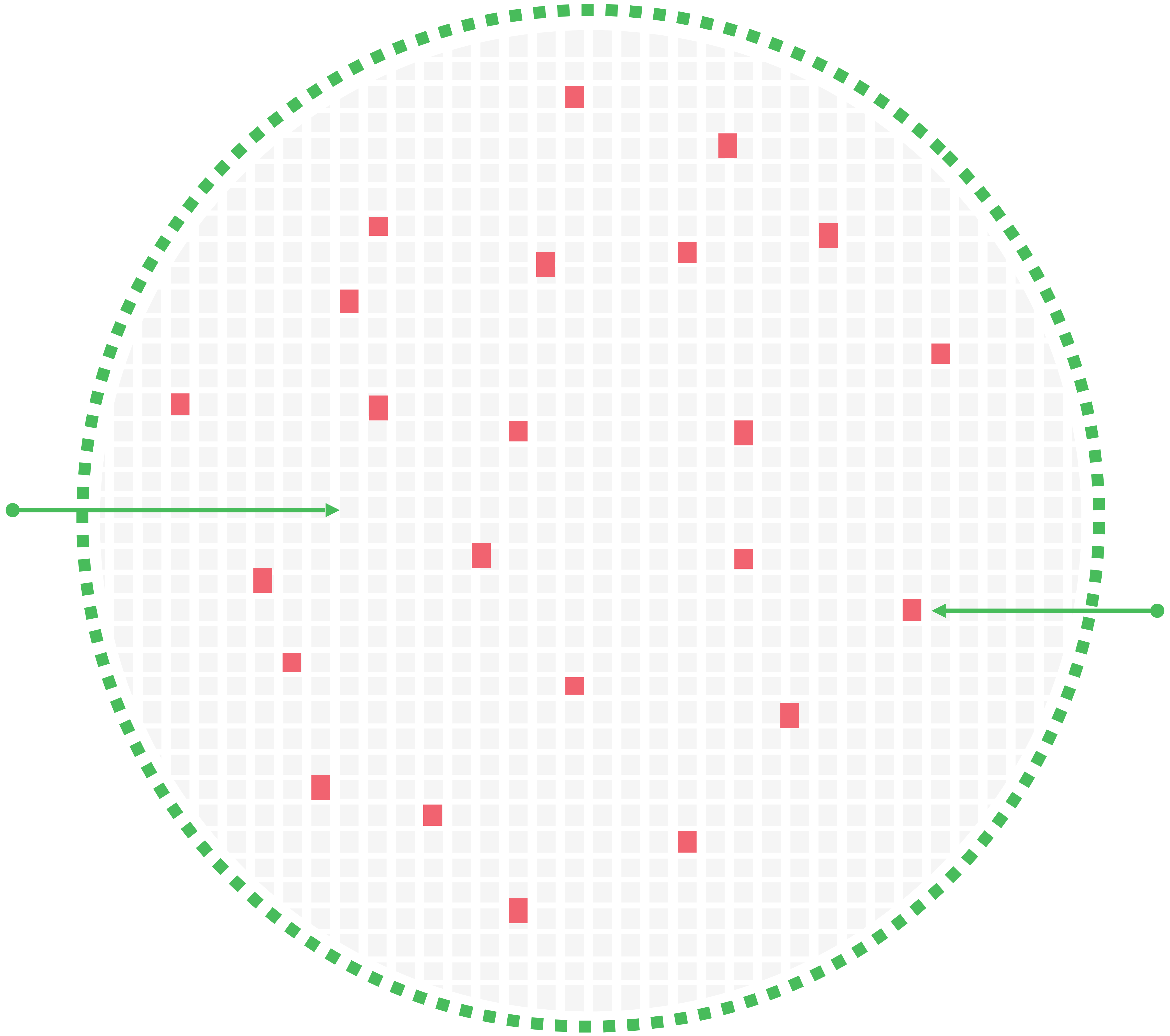
… **32** trojans

… **7** root enablers

… **4** surveillance

Threat encounter rate for **Healthcare** mobile devices

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



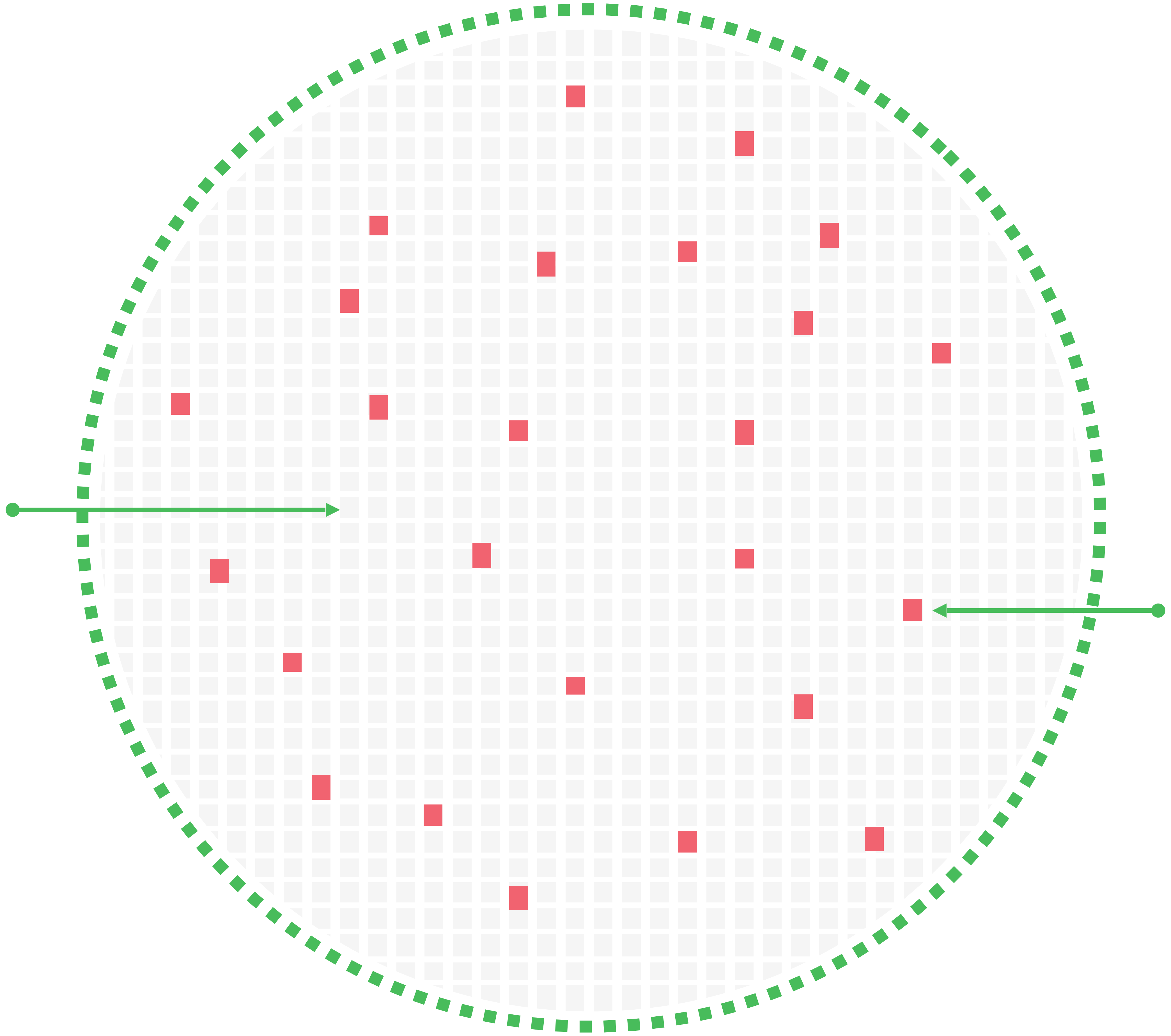
… **67** serious threats, of which

… **42** trojans

… **14** root enablers

… **7** surveillance

Threat encounter rate for **Financial Sector** mobile devices



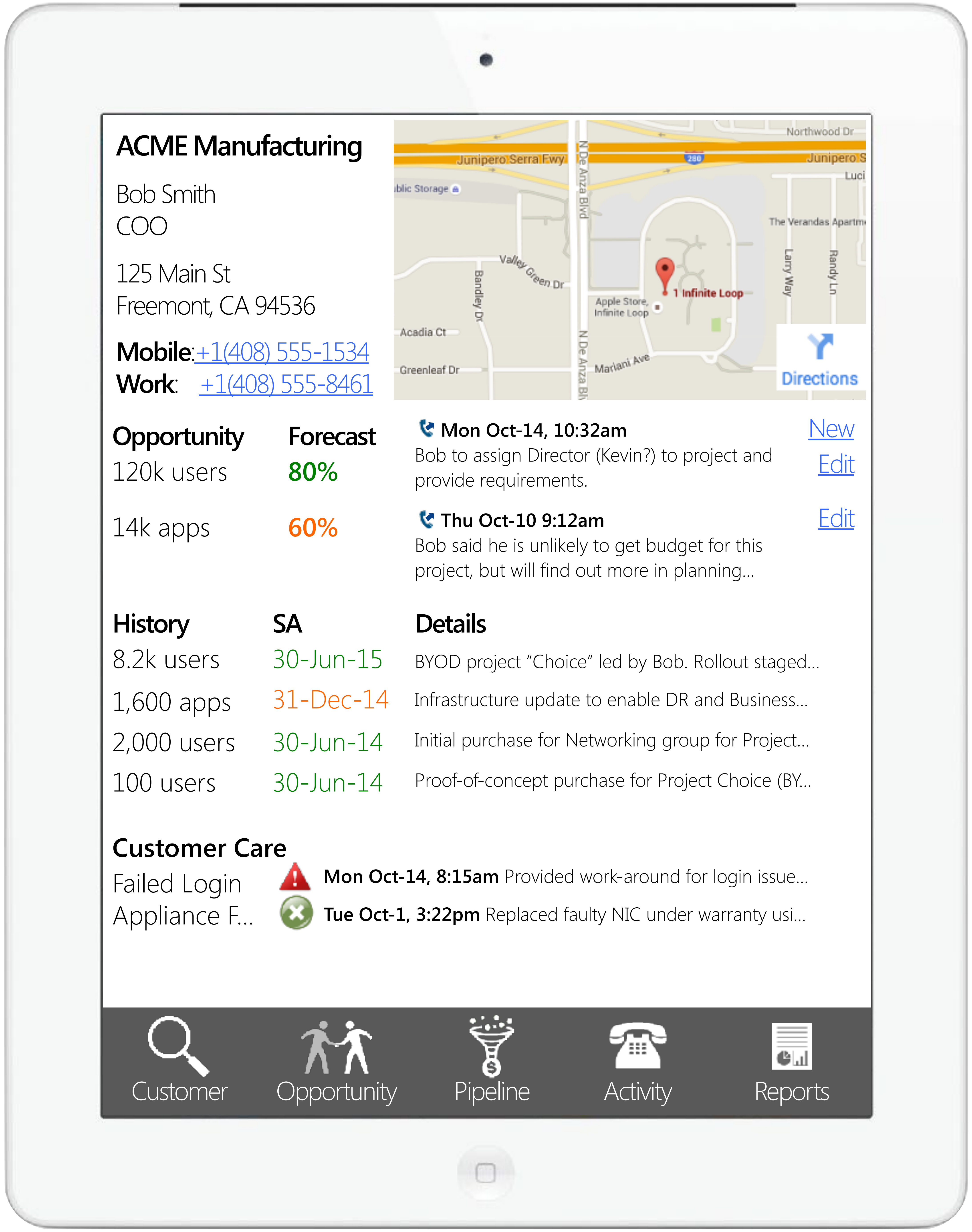
Out of every **1,000** enterprise mobile devices…

… **70** serious threats, of which

… **42** trojans

… **14** root enablers

… **8** surveillance



ACME Manufacturing

Bob Smith
COO

125 Main St
Freemont, CA 94536

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

Opportunity	**Forecast**
120k users	80%
14k apps	60%

☎ **Mon Oct-14, 10:32am**
Bob to assign Director (Kevin?) to project and provide requirements.

New
Edit

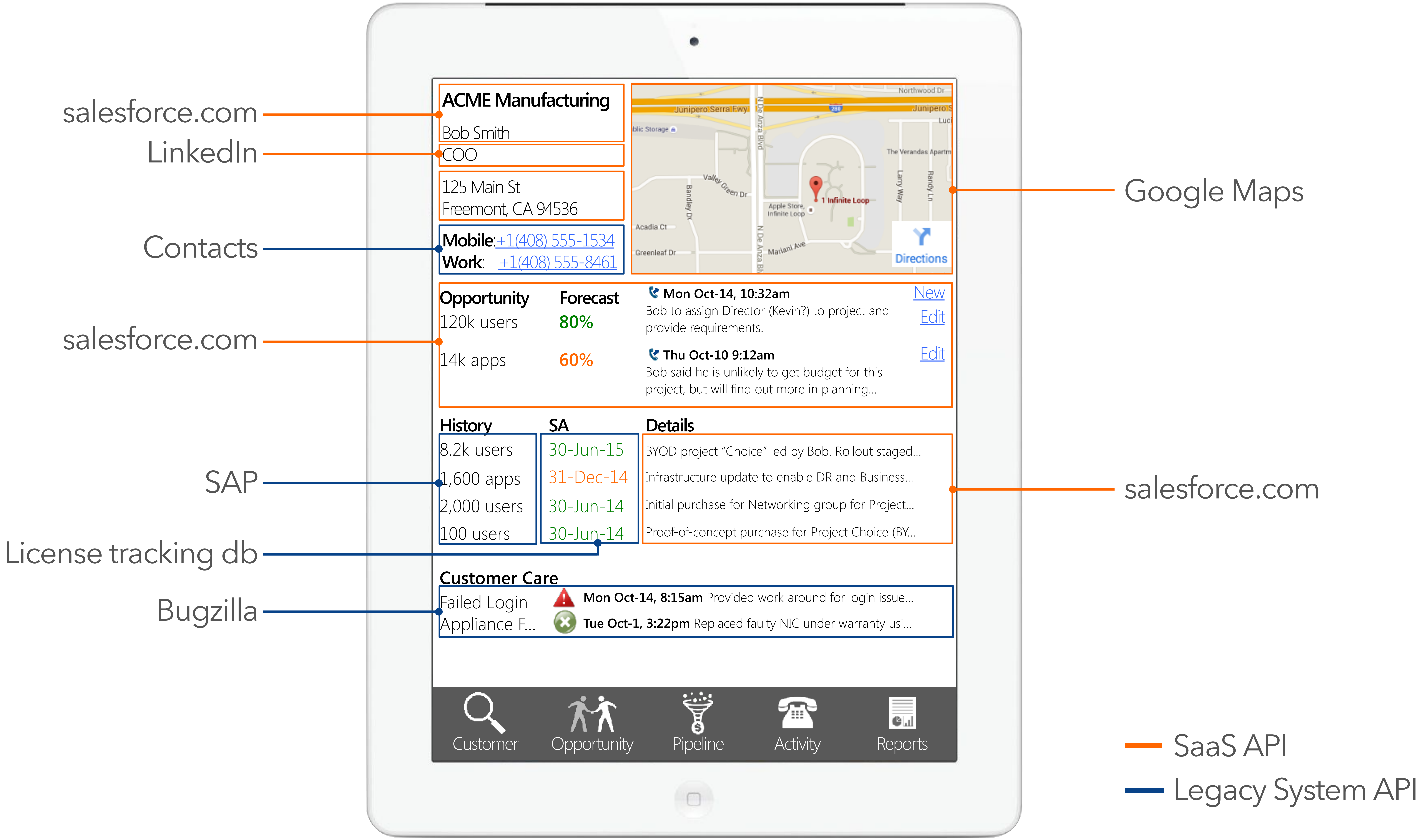
☎ **Thu Oct-10 9:12am**
Bob said he is unlikely to get budget for this project, but will find out more in planning…

Edit

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	⚠	**Mon Oct-14, 8:15am** Provided work-around for login issue…
Appliance F…	☒	**Tue Oct-1, 3:22pm** Replaced faulty NIC under warranty usi…



salesforce.com

LinkedIn

Contacts

salesforce.com

SAP

License tracking db

Bugzilla

Google Maps

salesforce.com

SaaS API

Legacy System API

ACME Manufacturing

Bob Smith

COO

125 Main St
Freemont, CA 94536

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

Opportunity	**Forecast**
120k users	80%
14k apps	60%

☎ **Mon Oct-14, 10:32am** New Edit
Bob to assign Director (Kevin?) to project and provide requirements.

☎ **Thu Oct-10 9:12am** Edit
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...

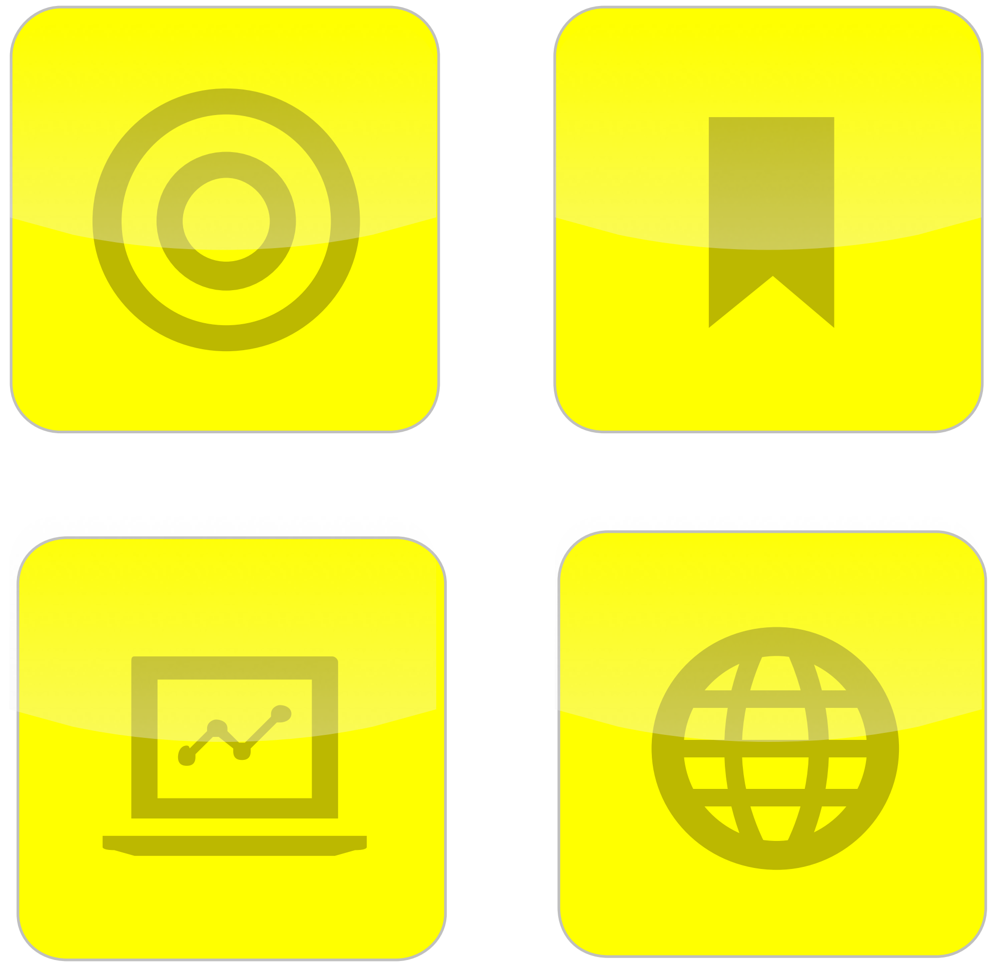
Customer Care

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

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

App behavior risk spectrum

Exhibits no sensitive behaviors

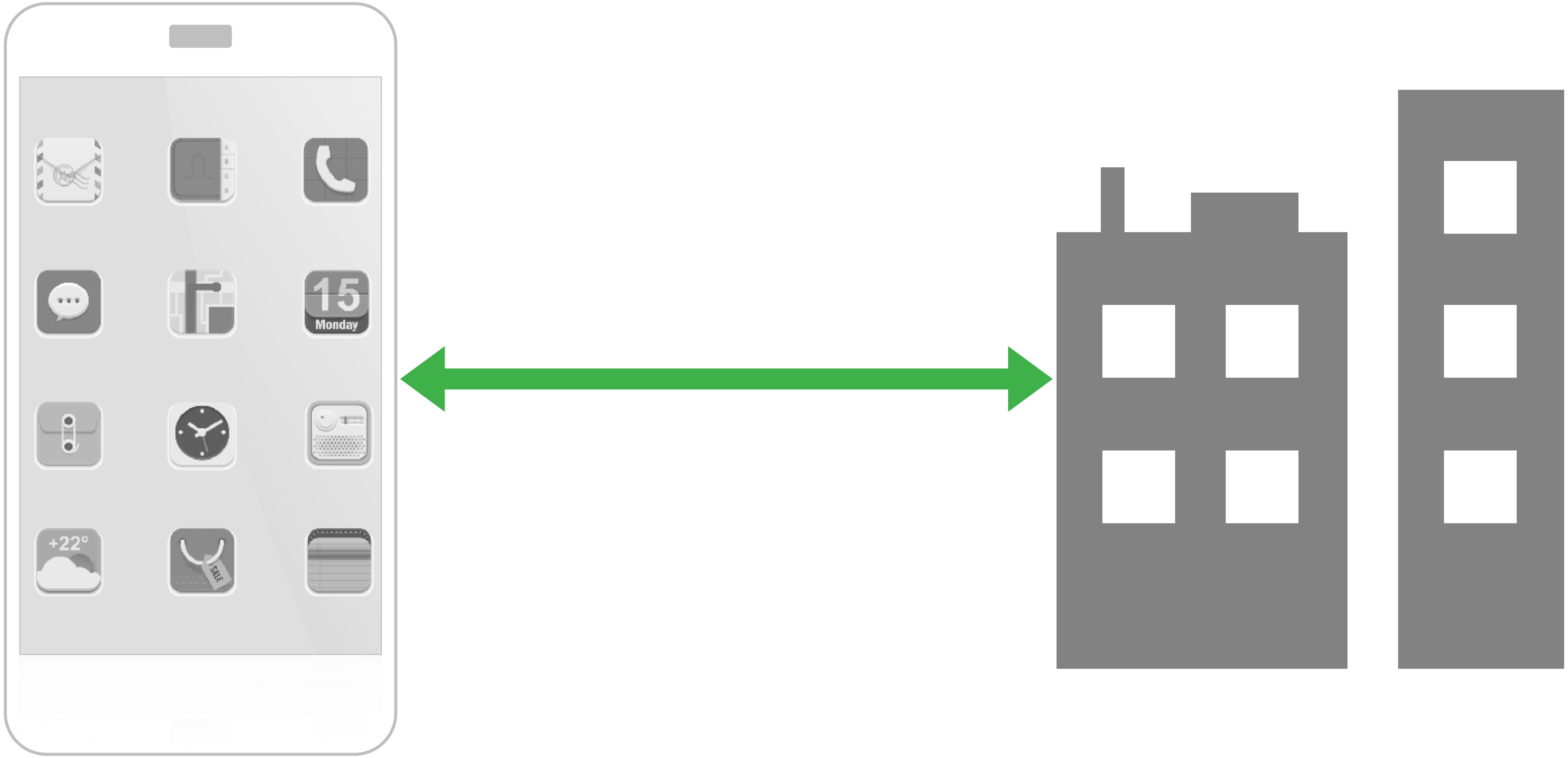


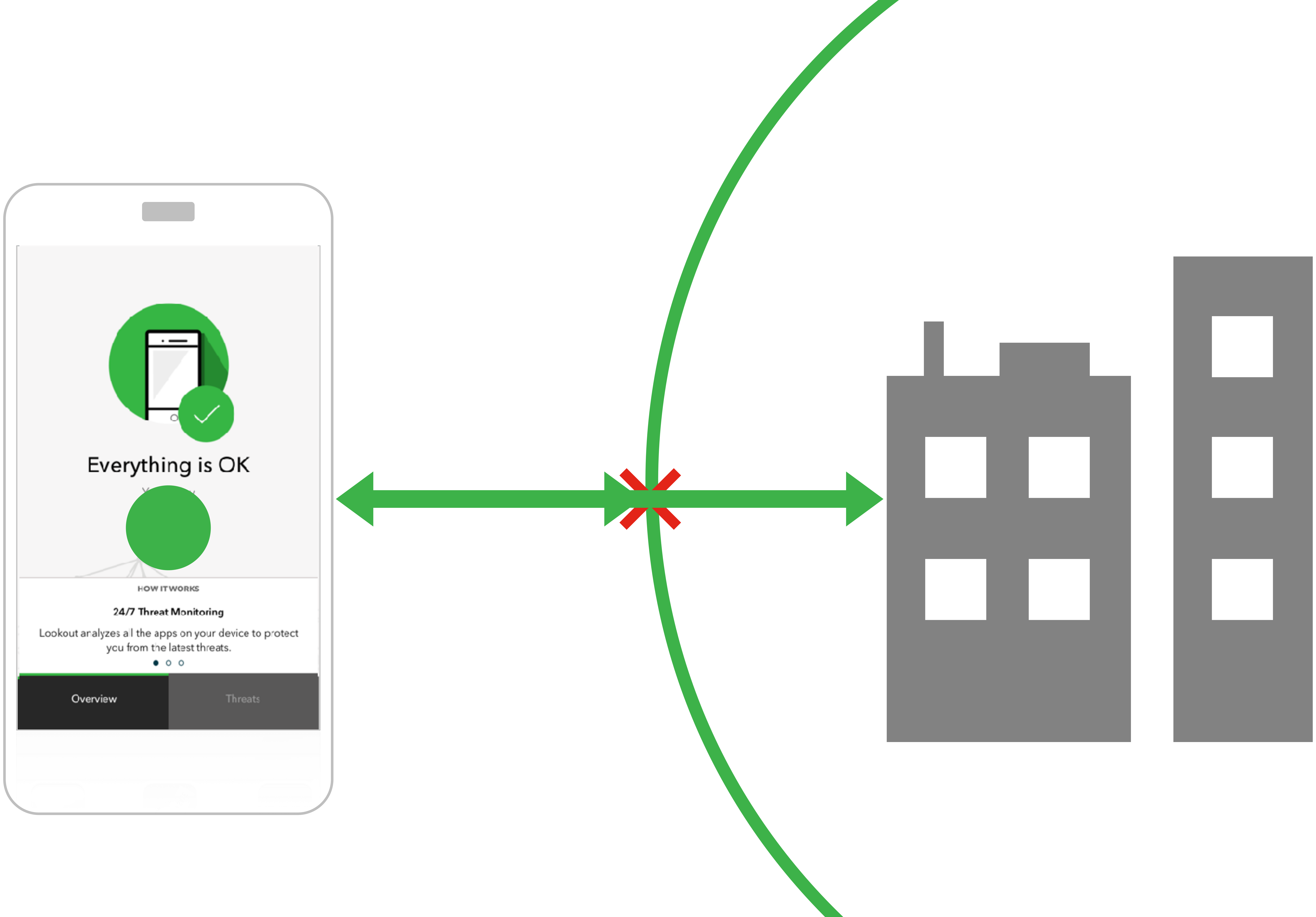
Exhibits one or more sensitive behaviors

Exhibits malicious behaviors

Protecting mobile devices requires a different approach

<API>


15
Monday
+22°
SALE

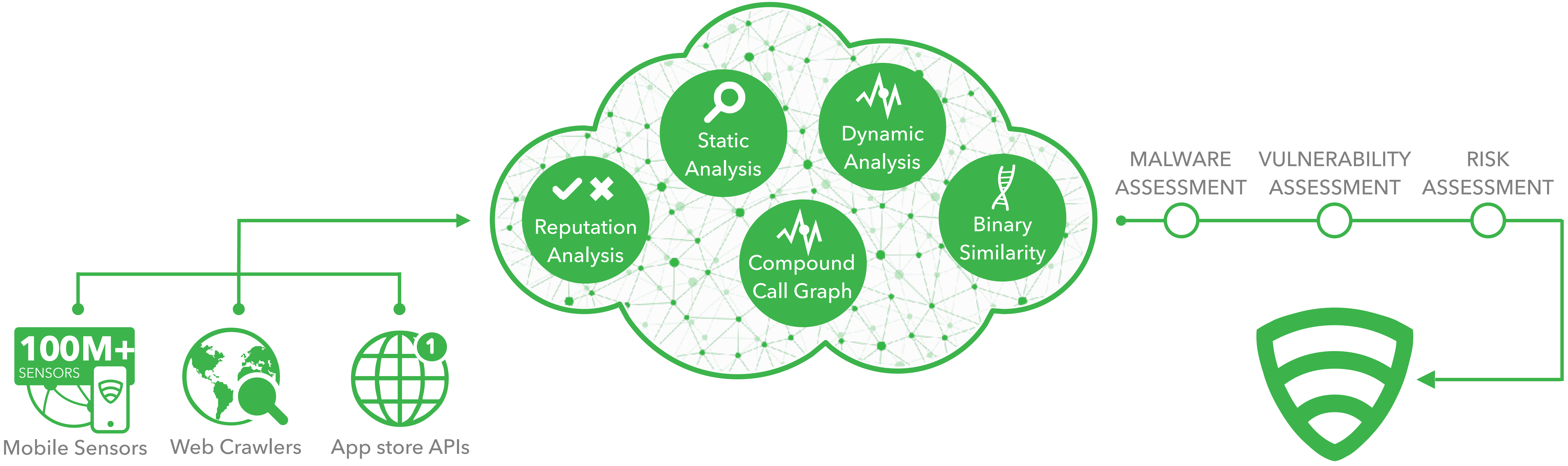


Everything is OK

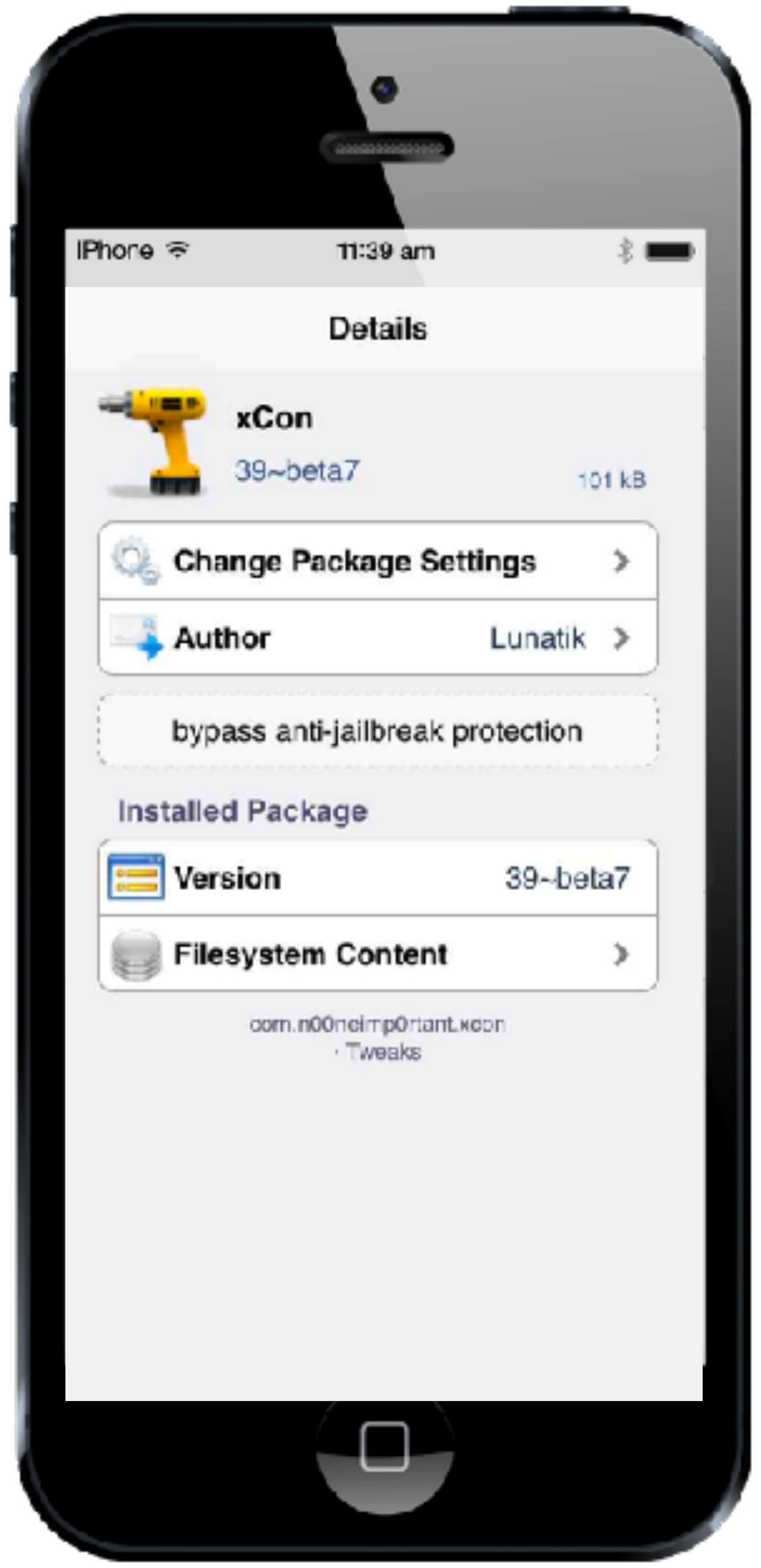
HOW IT WORKS

24/7 Threat Monitoring

Lookout analyzes all the apps on your device to protect you from the latest threats.



EVERYTHING WILL BE OK



iOS 9.3.5

iOS 10.0.1

jailbreak