wandera

Mobile Security Strategies in a Zero-Trust World:

PROTECTING USERS, DEVICES, APPS, AND DATA

SUZAN SAKARYA.
SALES DIRECTOR, UK&I

The borderless enterprise has arrived

Mobile endpoints have taken over

57% of enterprise Internet usage is over mobile (StatCounter)

Enterprise data is moving to the cloud

83% of enterprise workloads will be in the cloud by 2020 (Forbes)

Mobility enhances employee productivity

Support the devices that employees use

Make access easy (and secure)

Support the applications the business demands

salesforce
aws

Enabling the modern workplace

Access

Devices

Security

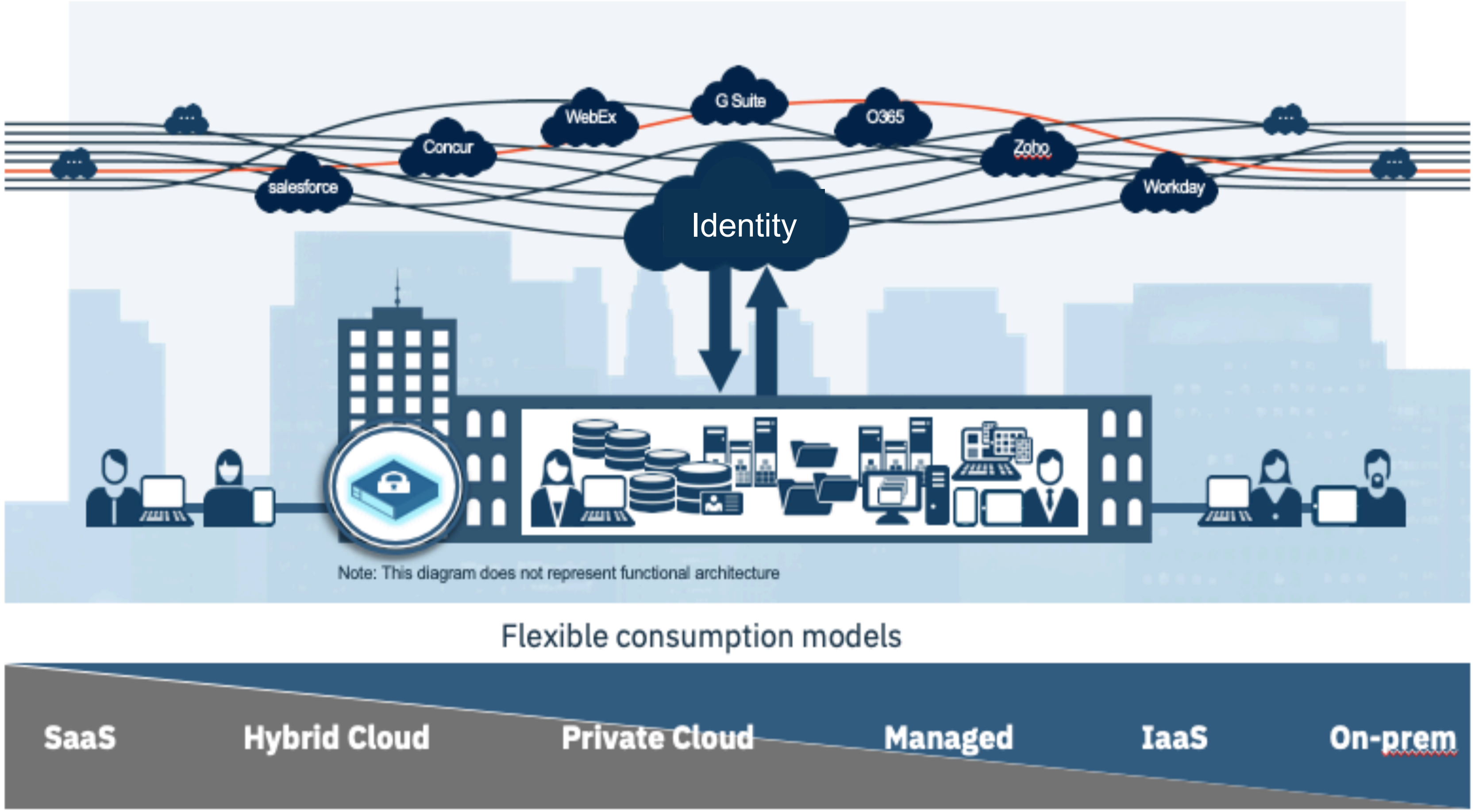
Enabling the modern workplace

Support end user productivity with **frictionless & secure access**

Devices

Security

Identity is essential to secure the borderless enterprise



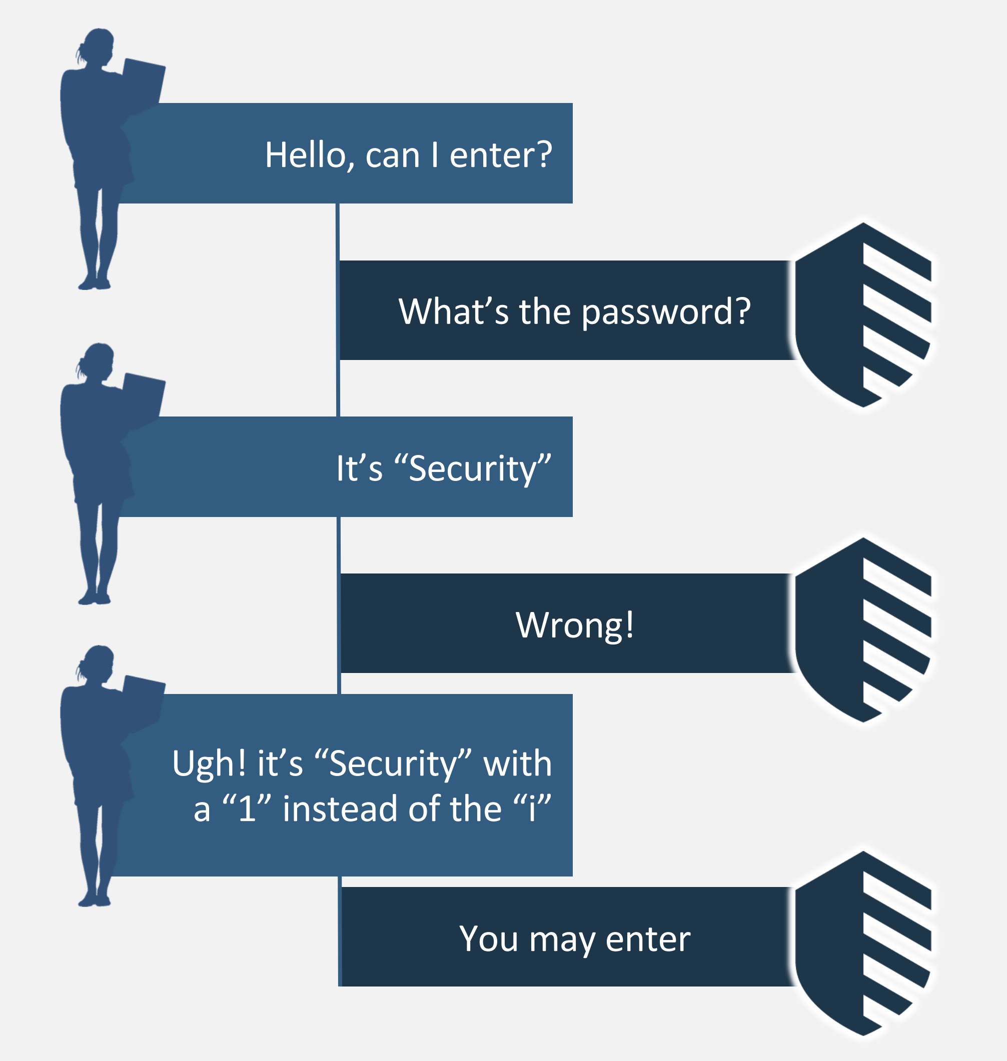
Note: This diagram does not represent functional architecture

Flexible consumption models

SaaS Hybrid Cloud Private Cloud Managed IaaS On-prem

Frictionless identity is key to enabling productivity

PASSWORD ONLY (older approach)



Hello, can I enter?

What’s the password?

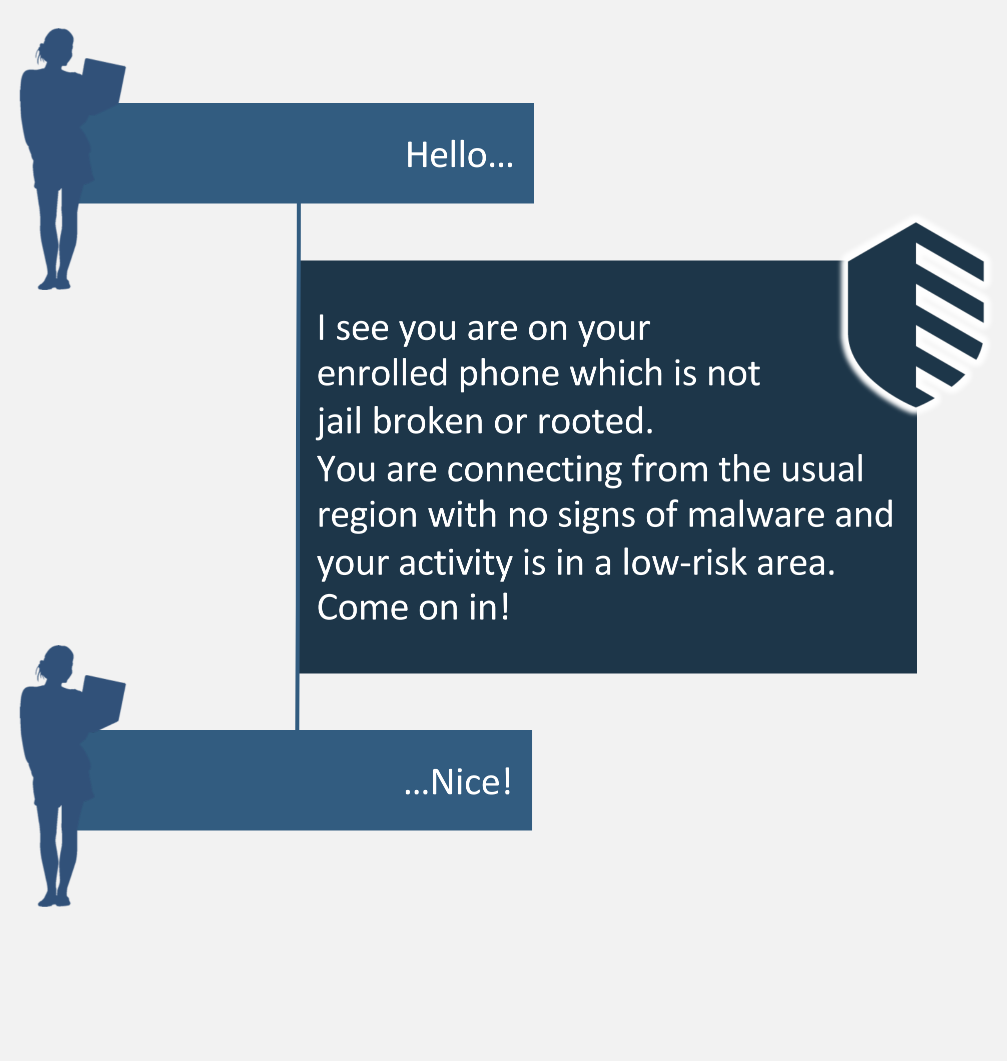
It’s “Security”

Wrong!

Ugh! it’s “Security” with a “1” instead of the “i”

You may enter

Silent Security Approach



Hello…

I see you are on your enrolled phone which is not jail broken or rooted.
You are connecting from the usual region with no signs of malware and your activity is in a low-risk area.
Come on in!

…Nice!

Enabling the modern workplace

Support end user productivity with **frictionless & secure access**

Devices

Security

Should access be allowed from *any* device?

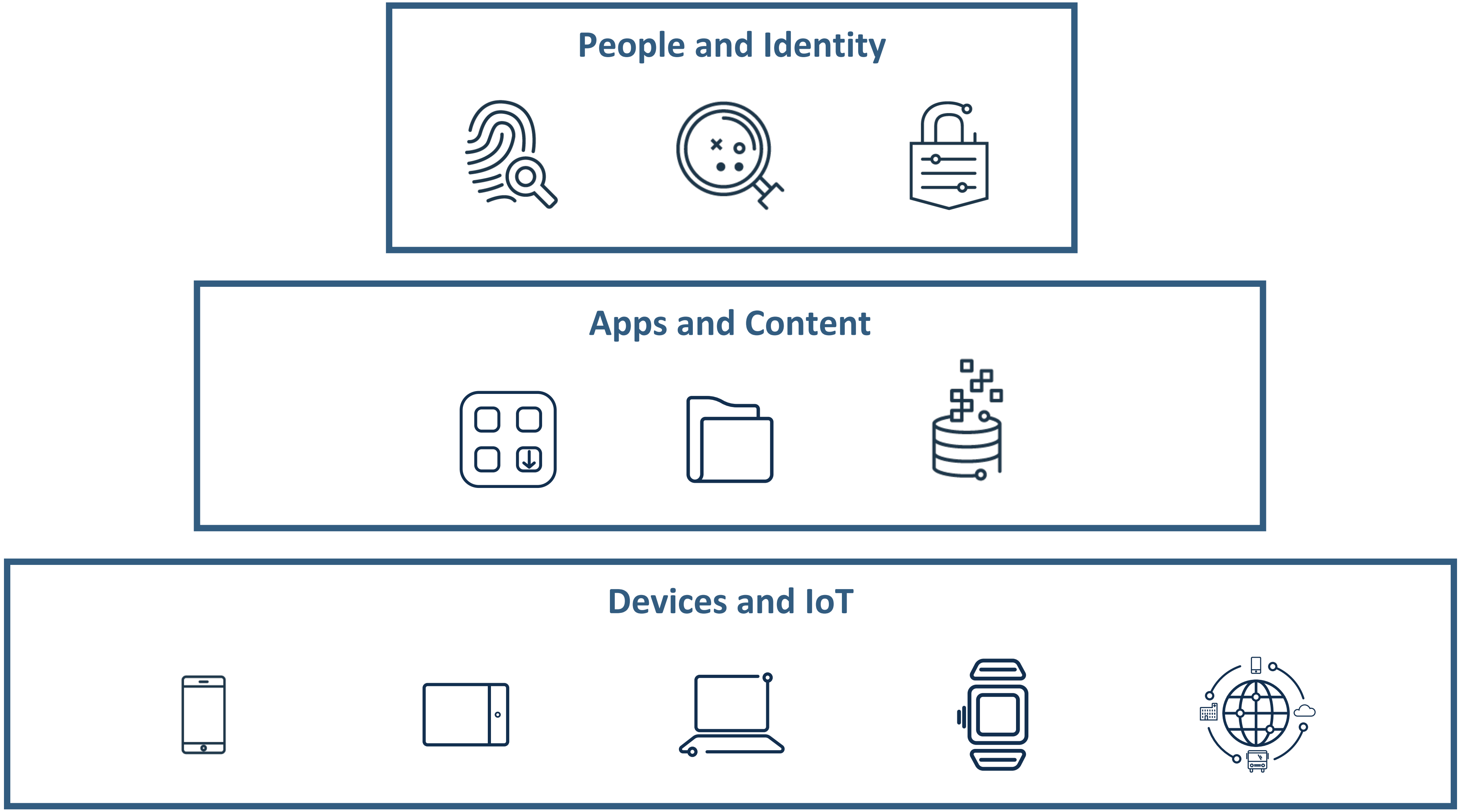
Enabling the modern workplace

Access

Consolidate resources by **managing any device** type and operating system

Security

Establishing a mobile-first management strategy



People and Identity

Apps and Content

Devices and IoT

Enabling the modern workplace

Access

Consolidate resources
by **managing any device** type
and operating system

Security

Are sanctioned device checks sufficient for security compliance?

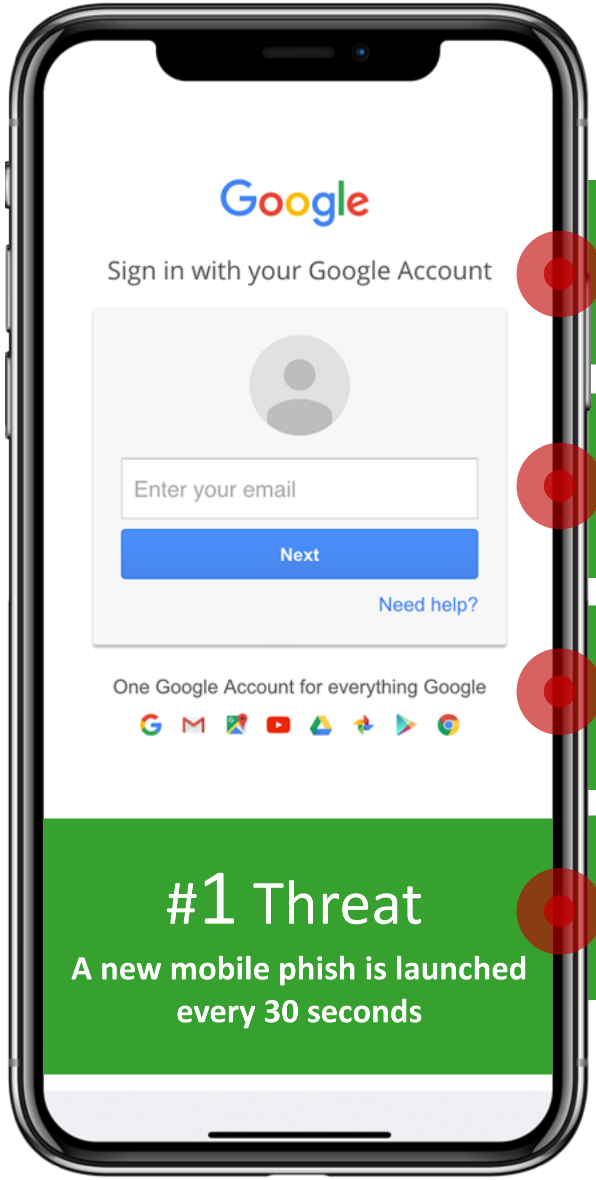
Enabling the modern workplace

Access

Devices

Protect endpoints & enterprise data with **best-in-class threat defense**

Mobile devices also introduce risk


Google
Sign in with your Google Account
Enter your email
Next
Need help?
One Google Account for everything Google

#1 Threat

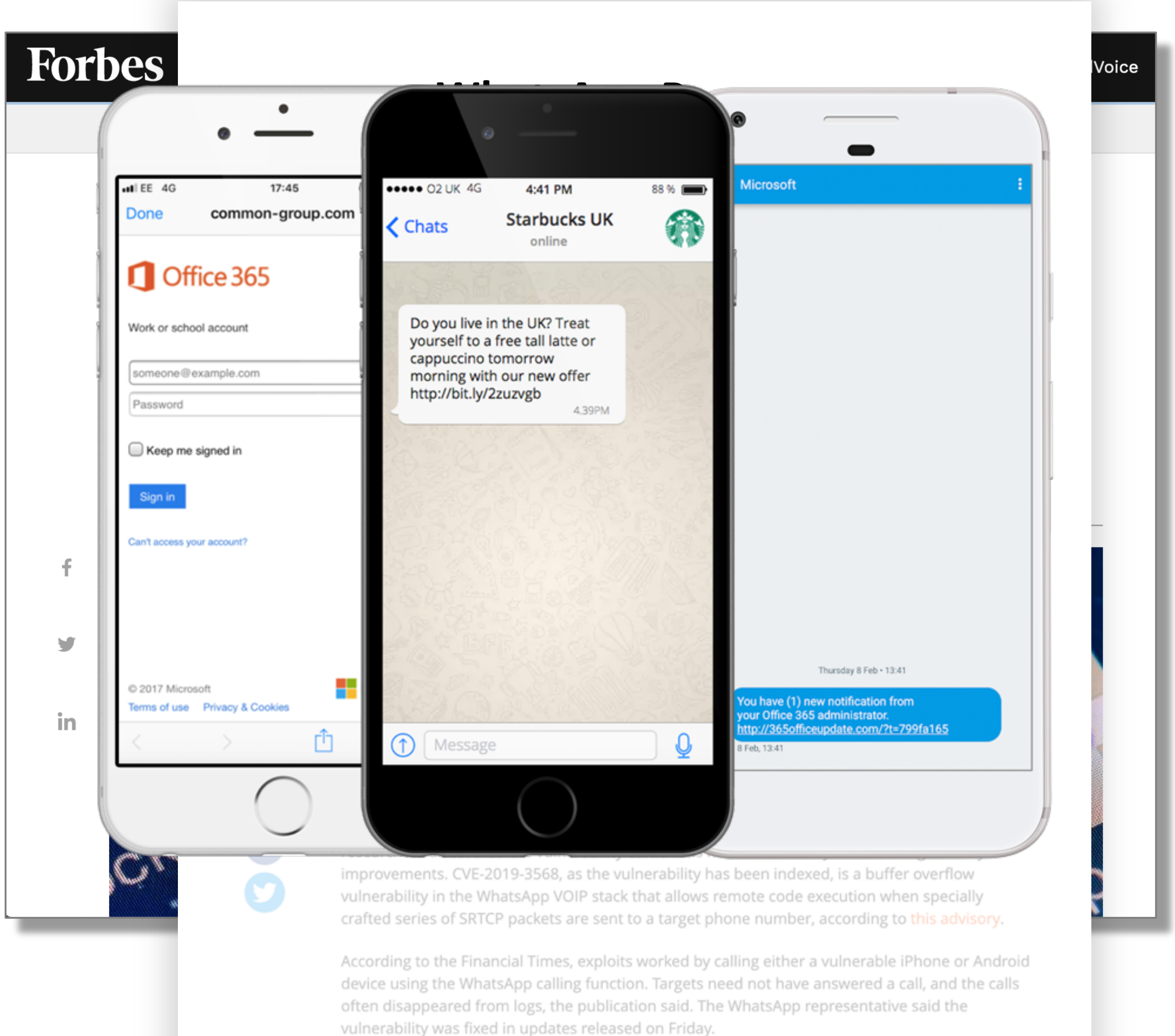
A new mobile phish is launched every 30 seconds

Device Risk

App Risk

Network Risk

Content Risk



Work or school account

someone@example.com

Password

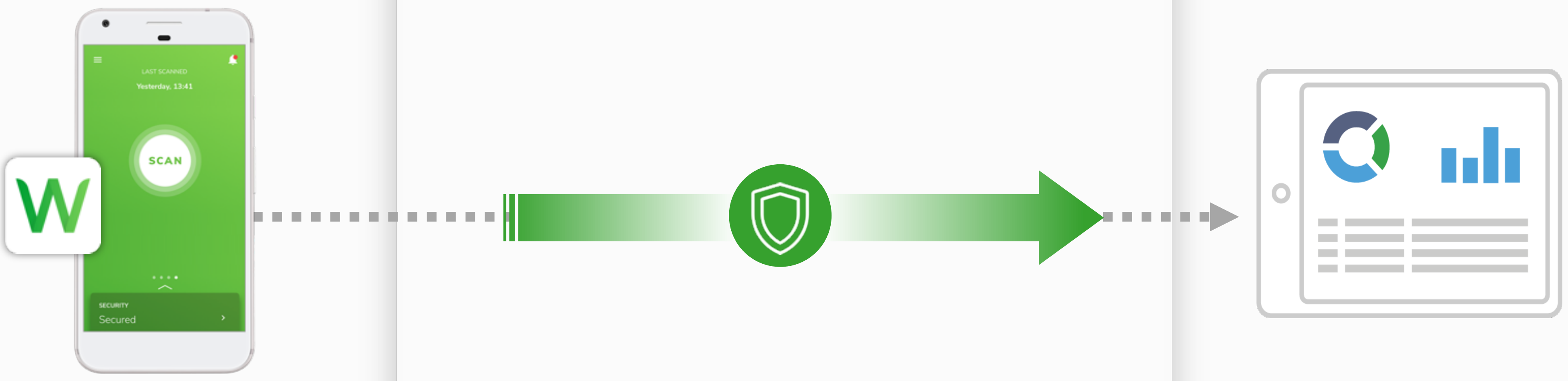
Do you live in the UK? Treat yourself to a free tall latte or cappuccino tomorrow morning with our new offer http://bit.ly/2zuzvgb

You have (1) new notification from your Office 365 administrator. http://365officeupdate.com/?t=799fa165

improvements. CVE-2019-3568, as the vulnerability has been indexed, is a buffer overflow vulnerability in the WhatsApp VOIP stack that allows remote code execution when specially crafted series of SRTCP packets are sent to a target phone number, according to this advisory.

According to the Financial Times, exploits worked by calling either a vulnerable iPhone or Android device using the WhatsApp calling function. Targets need not have answered a call, and the calls often disappeared from logs, the publication said. The WhatsApp representative said the vulnerability was fixed in updates released on Friday.

Establishing a secure foundation with Mobile Threat Defense



Endpoint Application

Any mobile device

- Vulnerability assessment
- App vetting
- Network threat detection
- Malware detection

Best-in-class detection

Network Suite

- Zero-day phishing prevention
- Web threat prevention
- Privacy-protected browsing
- MITM security

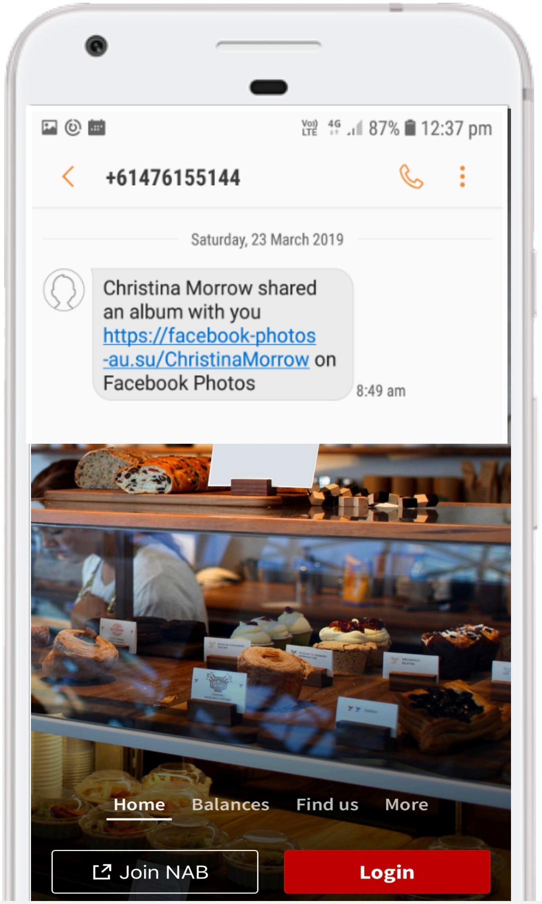
In-network prevention

Administrative Console

- Real-time security insights
- Incident investigations
- Policy controls
- Integrations (UEM, SIEM, IDP)

Enterprise-grade manageability

Case study: Protecting mobile workers



+61476155144

Saturday, 23 March 2019

Christina Morrow shared an album with you https://facebook-photos-au.su/ChristinaMorrow on Facebook Photos 8:49 am

SMS from contact received with link
HTTPS://facebook-photos-au.su/ChristinaMorrow

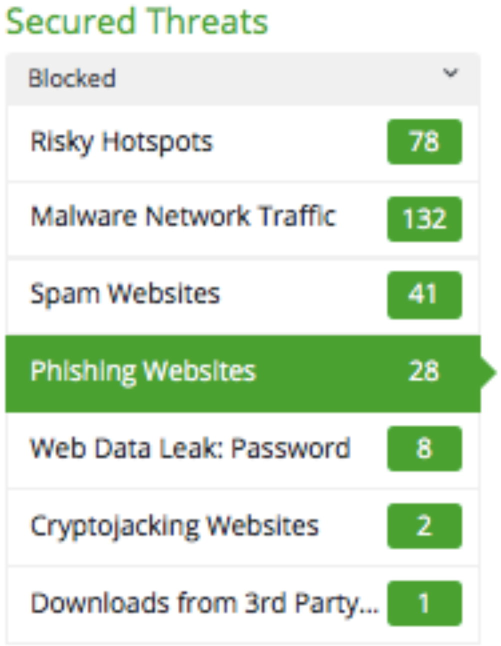
Steals contacts and sends SMS with victims name

Malware overlay imitates bank app and steals credentials

Captures SMS passcode to defeat 2FA

Disables traditional anti-virus software

VICTORIA
State
Government



Secured Threats

Blocked	
Risky Hotspots	78
Malware Network Traffic	132
Spam Websites	41
Phishing Websites	28
Web Data Leak: Password	8
Cryptojacking Websites	2
Downloads from 3rd Party...	1

Wandera Mobile Security Suite protected mobile workers by preventing attack

Holistic security for the modern workplace

Secure your mobile devices

- Protect the data
- Prevent spying

Secure connections over the network

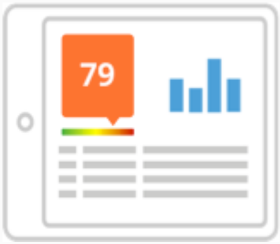
- Protect data in transit
- Prevent web threats

Secure your cloud applications

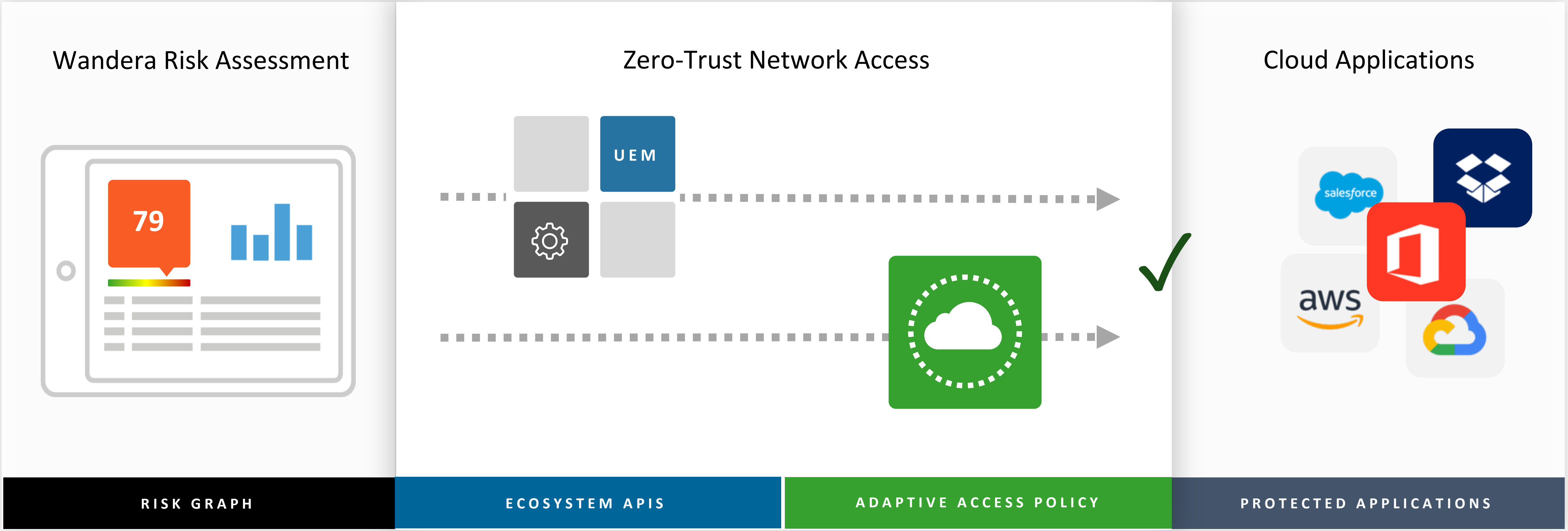
- Apply conditional access to your data
- Continuously monitor for risk

Wandera Risk Graph

Powered by MI:RIAM



Trusted Mobile Access: ZTNA Solution for Cloud Access



Wandera Risk Assessment

Zero-Trust Network Access

Cloud Applications

RISK GRAPH

ECOSYSTEM APIS

ADAPTIVE ACCESS POLICY

PROTECTED APPLICATIONS

Enabling the modern workplace

Support end user
productivity with
frictionless & secure access

Consolidate resources
by **managing any device** type
and operating system

Protect endpoints & enterprise
data with
best-in-class threat defense

Effective protection requires a multi-layer approach

Gartner

2018 Market Guide for Mobile Threat Defense

- Full checkmarks across all threat capabilities
- Largest number of UEM/SIEM integrations
- Identified as only multi-level provider

IDC

Worldwide Mobile Threat Management Software 2018-2019

- Recognized as a **Leader**
- Highest rating in customer satisfaction
- Recognized for in-network capabilities

SC 2017 awards EUROPE Winner

Computing Security Awards

wandera

MOBILE SECURITY
IN PERFECT BALANCE

For the Enterprise	For mobile workers
› Manage all aspects of mobile risk	› Protect user identity
› Assess risk on device and in the network	› Enable seamless access and usable security
› Protect application data, at rest and in transit	› Secure mobile usage, both business & personal
› Operationalize using ecosystem integrations	› Protect worker privacy; Enable productivity

wandera