



Modernes Arbeiten erfordert moderne Sicherheit

(EMM ein nützliches Werkzeug zur Einhaltung der DSGVO)

Manuel Melkonian
Channel Manager DACH & EE



MobileIron



It's Friday night.
Do you know where
your data is?

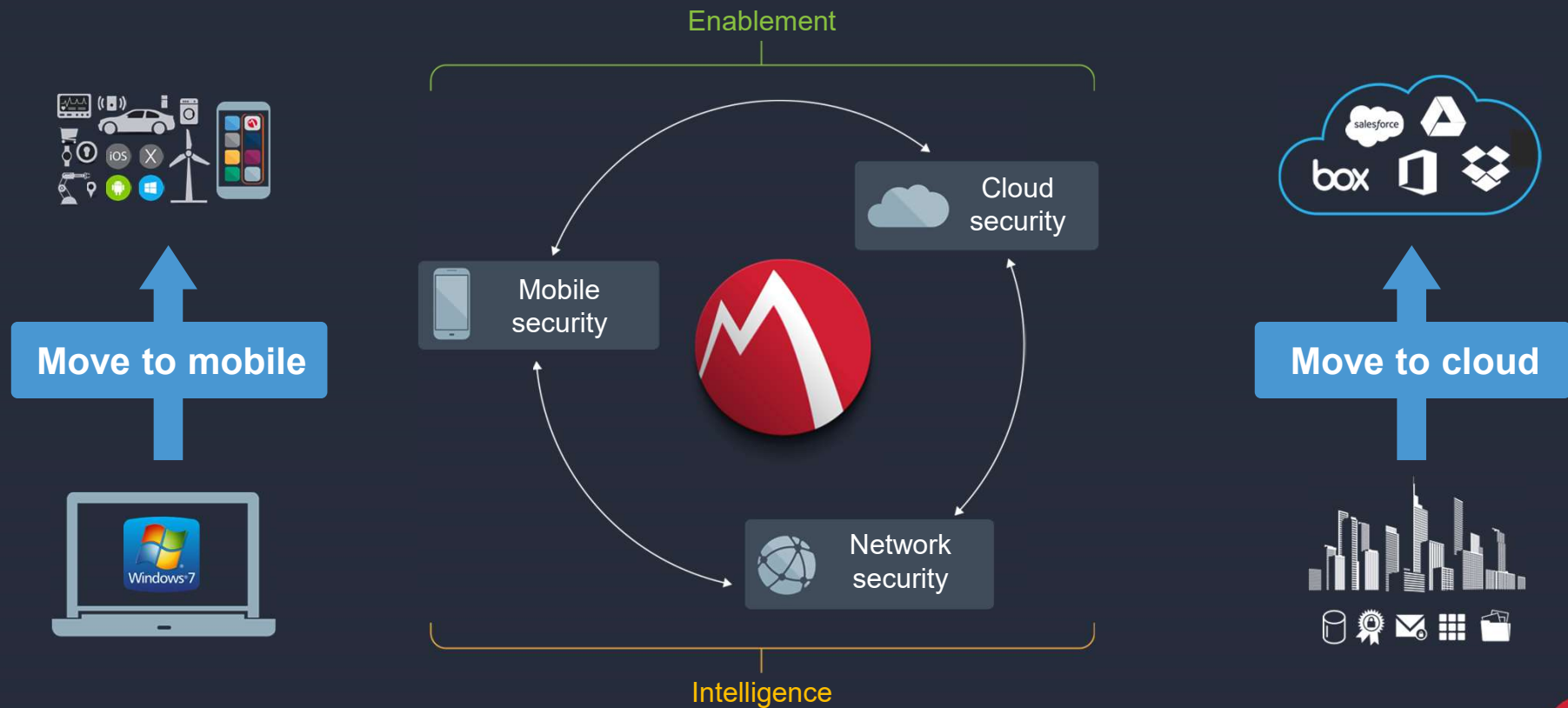
Data used to be here



Now it is everywhere



Two trends power the market



Cloud Security



Modern security & apps

Protect your data
@ the endpoint

EMM

Proactive Security
(Offense)



Threat

Reactive Security
(Defense)

Control where your
data is going

**Trusted
access**

Risk based Access Control /
AdvancedAppAnalytics for the Cloud



**Identity /
AAA**

Use your
data, be
productive

Apps

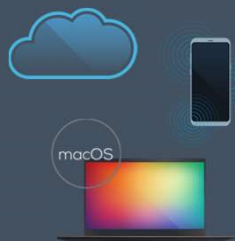
App adoption &
great user
experience

Policy & Analytics



Product Strategy

Protect data



100% adoption
Detect & Remediate

Control data



Context + Behavior Risk



SSO, No Password
Mobile Authenticator

Use data:



100% adoption
Secure Apps/BB Rip

Policy & Analytics

LOB Relevance
C-Level Relevance





MobileIron platform architecture

MobileIron security starts where the perimeter stops: human-centric, cross-stack, contextual

Trusted workspace

Unified policy


Trusted access


 **Apps@Work**
Enterprise app store

 **Email+**
Secure email

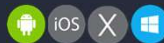
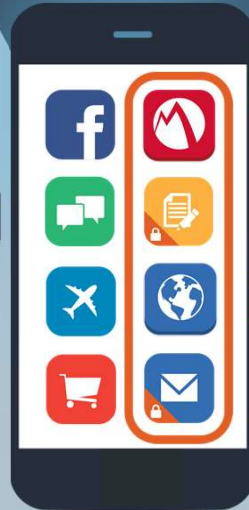
 **Docs@Work**
Secure content

 **Web@Work**
Secure browsing

 **Help@Work**
Troubleshooting

 **Tunnel**
Per app VPN

AppConnect
Ecosystem



END USERS



ENTERPRISE IT

Note: Some features will vary by device and deployment model



Broad, integrated ecosystem

Applications



Security

Services multiplier

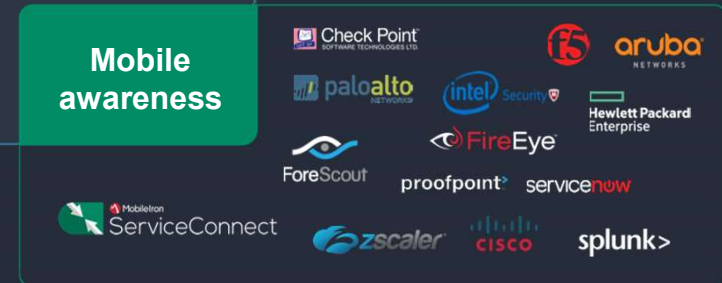


Service providers

OS/ODM



Device adoption



Mobile awareness

Infrastructure



SECURITY AUDIT

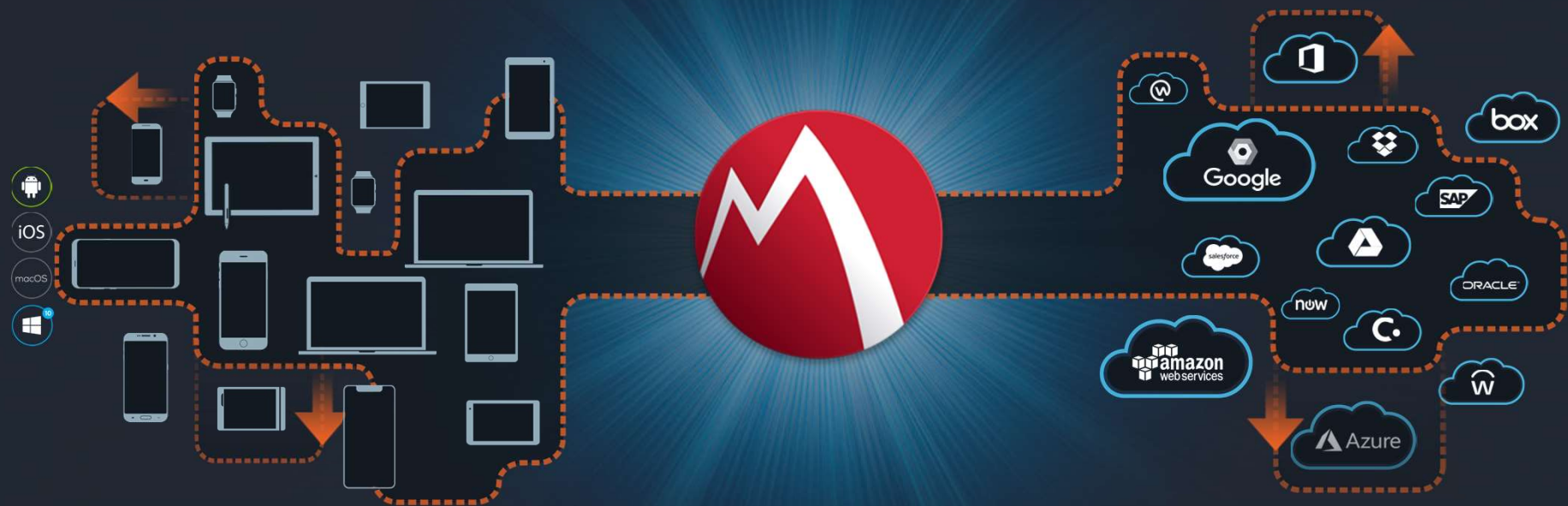
- ☐ Enforce device encryption and password protection
- ☐ Prevent business apps from sharing data with personal apps
- ☐ Automatically delete business data from compromised devices
- ☐ Tunnel business traffic without tunneling personal traffic
- ☐ Stop unauthorized devices and apps from accessing business cloud services
- ☐ Detect and remediate zero-day exploits
- ☐ Provide rich security controls for Android, iOS, macOS, Windows 10
- ☐ Certify for device and cloud security (Common Criteria, FedRAMP, SOC 2)

SECURITY AUDIT

- ☒ Enforce device encryption and password protection
- ☒ Prevent business apps from sharing data with personal apps
- ☒ Automatically delete business data from compromised devices
- ☒ Tunnel business traffic without tunneling personal traffic
- ☒ Stop unauthorized devices and apps from accessing business cloud services
- ☒ Detect and remediate zero-day exploits
- ☒ Provide rich security controls for Android, iOS, macOS, Windows 10
- ☒ Certify for device and cloud security (Common Criteria, FedRAMP, SOC 2)

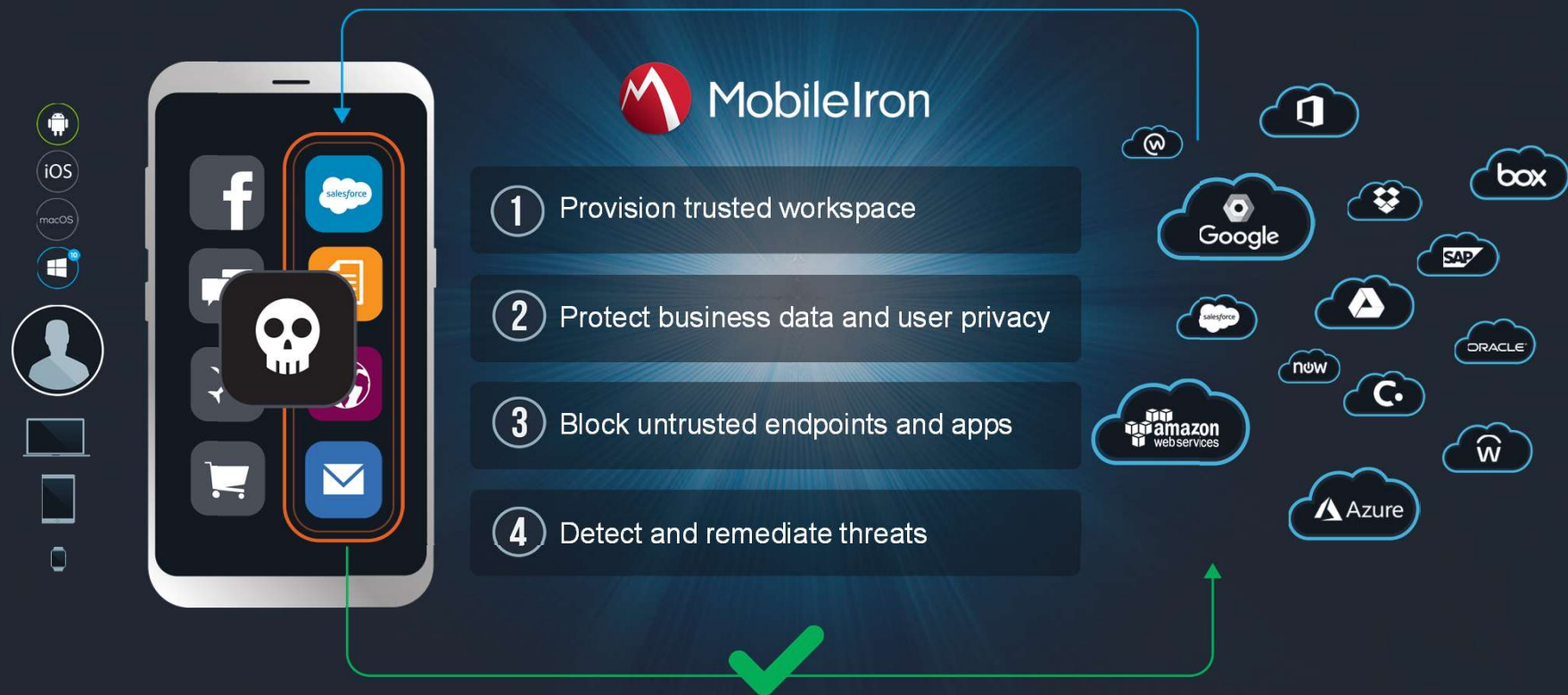


Modern security



Adaptive data perimeter

Seamless, secure experience from endpoint to cloud





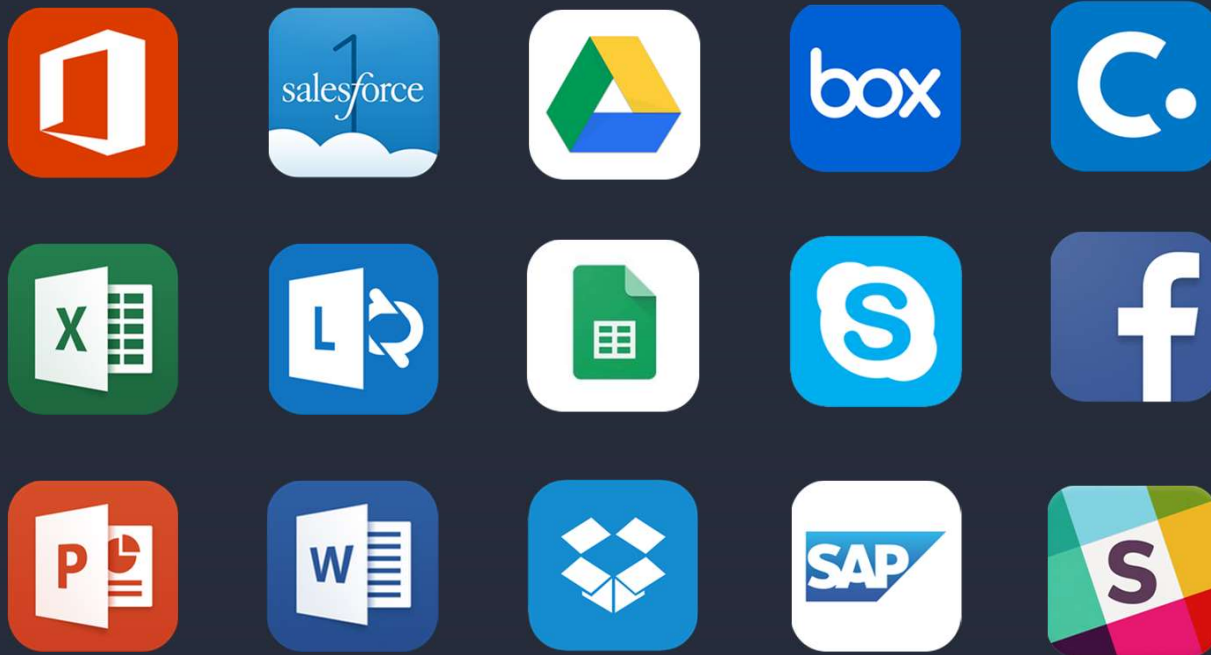
MobileIron
ACCESS

MobileIron Access



MobileIron

Popular apps used by employees



Source: CCS Insight



**90% of MobileIron
customers use one...**



Office 365



Salesforce



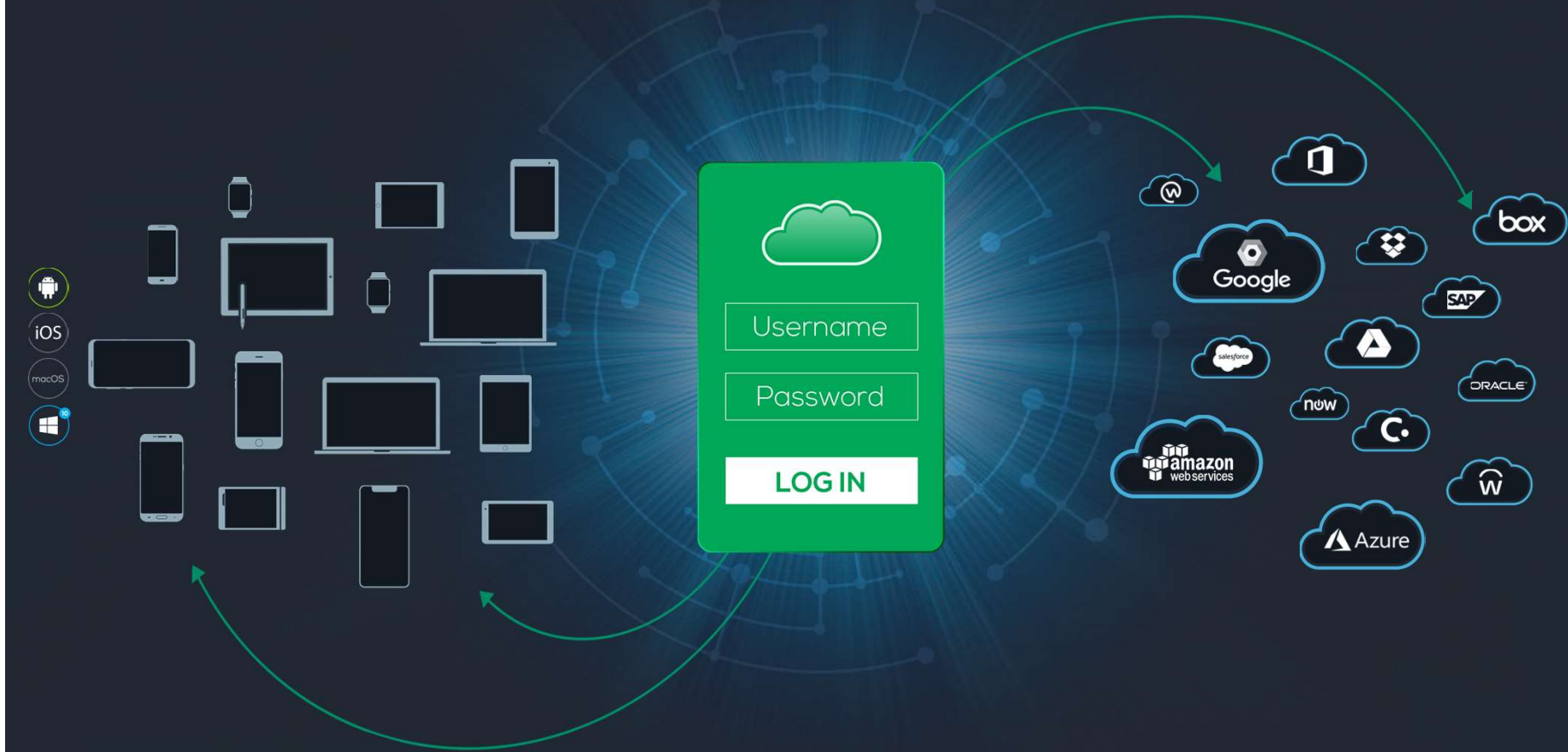
Google Apps



Box

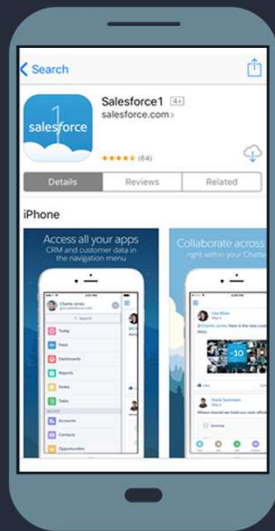


Can user identity secure your data?



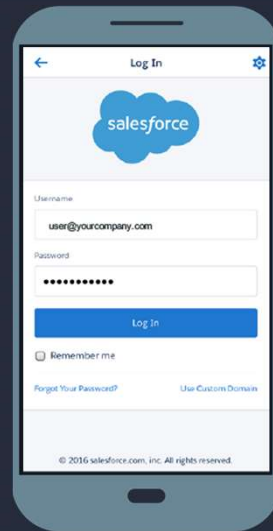
User identity alone cannot secure your data

1



Download

2



Sign in

Can you:

Delete app if device is lost?

NO

Prevent data sharing with consumer apps?

NO

Pass security audits (GDPR, NIST)?

NO

User identity is not enough



Risk vectors for mobile-cloud world

Data security:



Unsecured
devices



Unmanaged
apps



Unsanctioned
cloud services

Adoption:



Poor user
experience

Compliance:

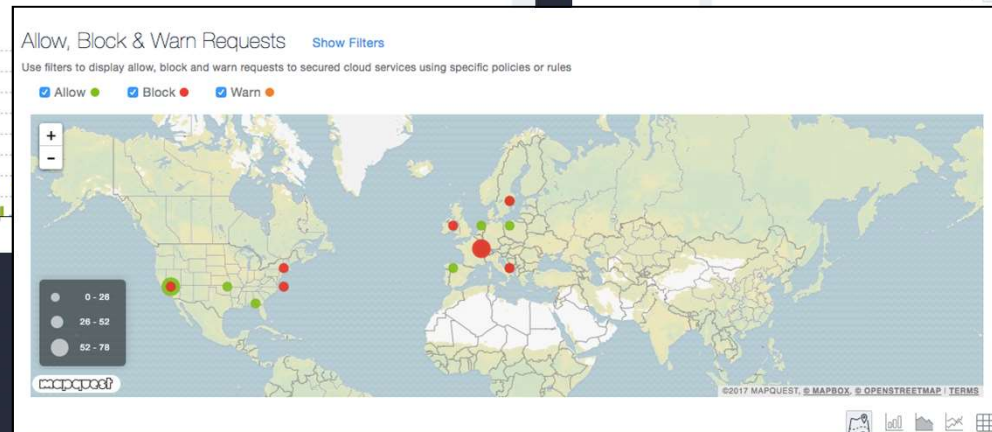
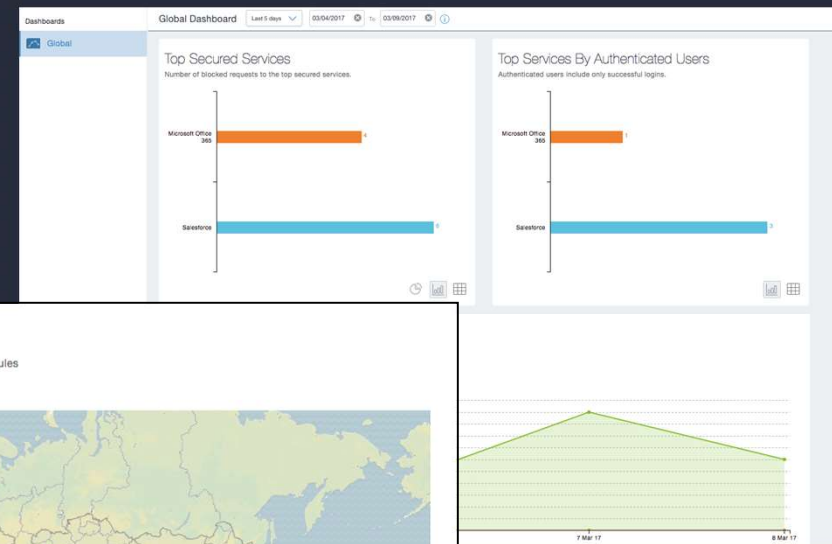
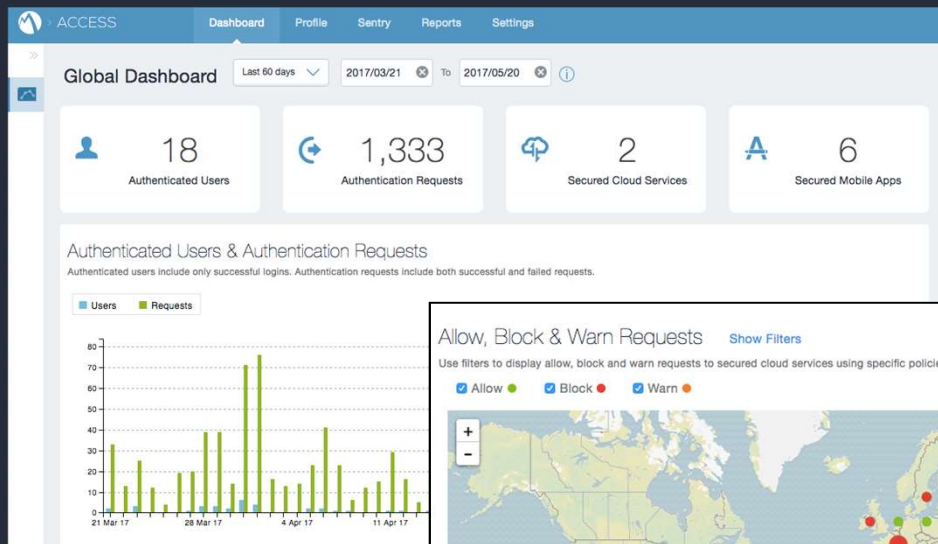


Visibility



Audit and discovery





Detailed audit logs



Contextual search





 MobileIron
ACCESS

Secure cloud services on mobile

**Protect business
data**

**Simplify
authentication**

**Get visibility for
compliance**





Cloud Security in Action



Biz Apps
(secured)

Biz Apps
(not secured)

Personal Apps &
Cloud Services



Conditional Access Approved

Conditional Access Denied



Standard
Authentication

No special App or Identity coding

- ? User ID?
- ? Secure Device?
- ? Secure App?



Customized Block Alert

XYZ CORP
Your access to this Cloud Application is blocked for security reasons. In order to securely access this Cloud Application, please use a properly secured mobile device and download apps from [Company Name] enterprise app store.
Go to the [Help Center Link] for more information or contact the helpdesk at [Help Center Email]





MobileIron
**THREAT
DEFENSE**

MobileIron Threat Defense

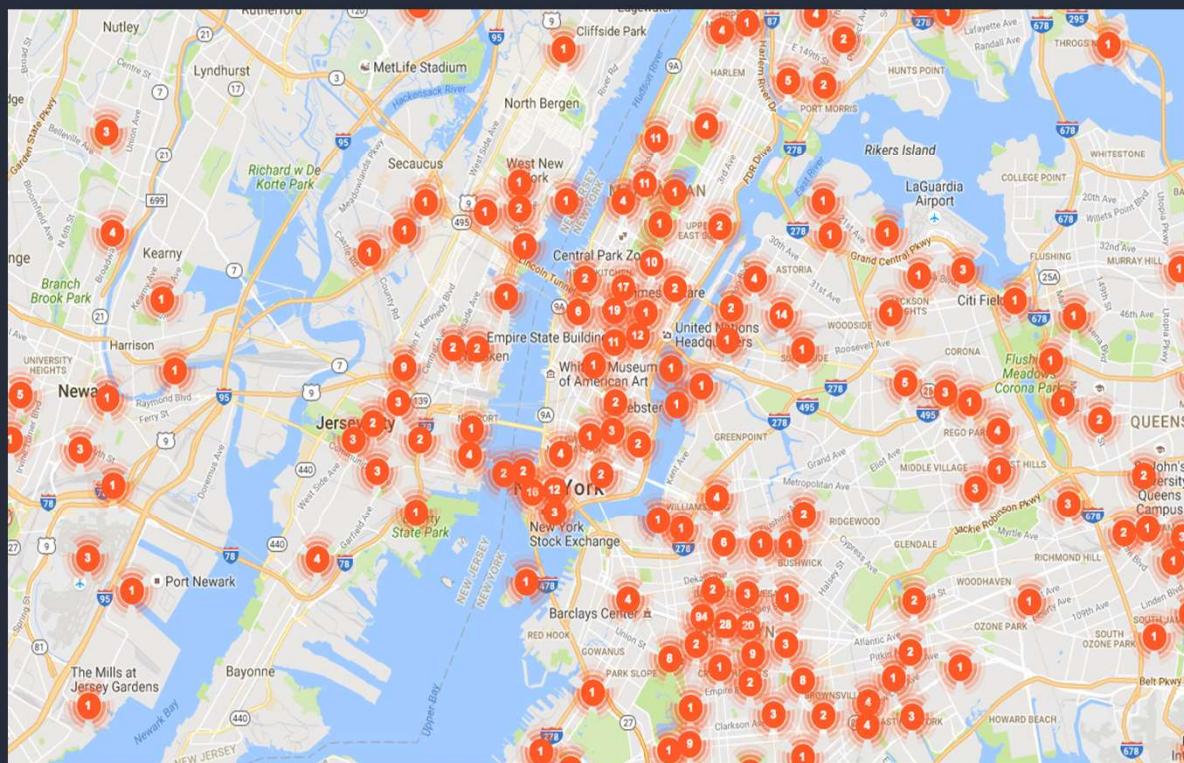


MobileIron

Mobile threats are everywhere

24% Of organizations suffered a mobile security attack, primarily driven by malware & malicious WiFi

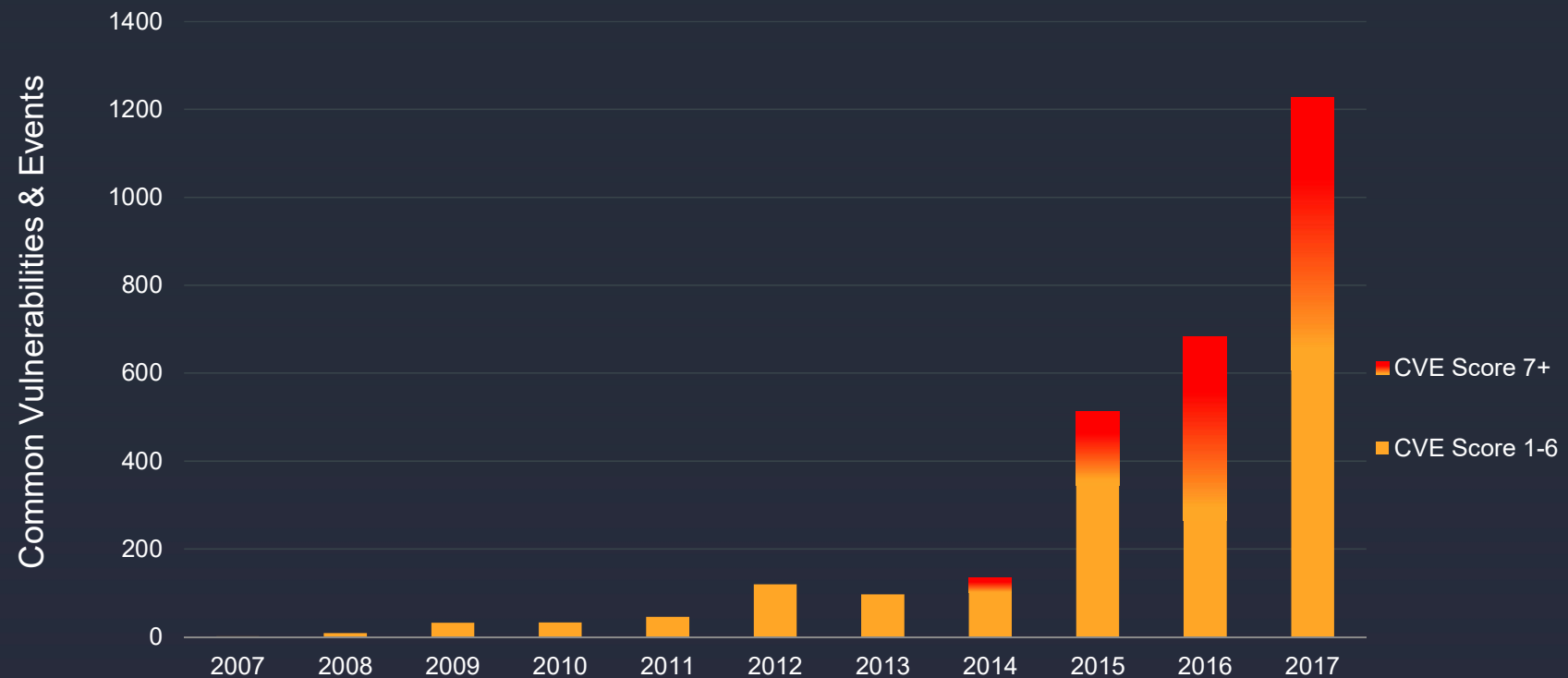
43% Were unsure if mobile security incidents had occurred



Source: 2017 Mobile Security Report, Zimmerium



Risk is escalating rapidly



Source: CVE.Mitre.org, CVEDetails.com: Android and iOS CVEs



Mobile attacks are not created equally

The sole objective
for persistent
foothold



Device
attacks

The primary
mechanism for
targeted attacks



Network
attacks

Untargeted,
advertising & fraud
threats



Application
attacks



Detect & remediate on-device, no user action

Easy



1 app

No user action required

Insightful



Immediate and
ongoing visibility

Risky app analyses

On-Device



Zero-day detection &
remediation on-device

No connectivity

Machine learning





Provision trusted workspace

with advanced authentication and single sign-on across apps for a powerful native experience



MobileIron Confidential





Protect business data and user privacy

by isolating business from personal data on endpoint and across network



MobileIron Confidential





Block untrusted endpoints and apps

by enforcing adaptive access across cloud and on-premises services



MobileIron Confidential





Detect and remediate threats

across device, network, and app (DNA) using machine learning and on-device enforcement



MobileIron

MobileIron Confidential



