mobileiron
The center of enterprise security

Zero sign-on:

passwordless authentication for the multi-cloud enterprise

Claus Nussbaum
Director Austria & Eastern Europe

AGENDA

- Passwords cause breaches
- Zero sign-on experience
- Platform & product overview
- Key takeaways

mobileiron

mobileiron

A proven mobile leader

19,000 Customers

11,000,000 Business critical endpoints

80+ Security patents

105% Revenue renewal rate

350+ Ecosystem partners

9x Gartner leaders quadrant

2019 Recognition:

Gartner peerinsights customers' choice 2018

FORRESTER Wave Leader

IDC

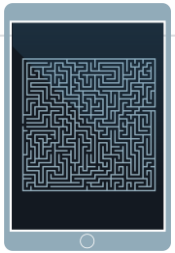
SCP SERVICE CAPABILITY & PERFORMANCE - CERTIFIED -

Passwords result in data breaches

Organizations are in a no-win situation

85%

said their businesses face at least a moderate risk from mobile security threats*



32%

admitted to having sacrificed mobile security to improve expediency and/or business performance*

$3.6M

is the average total cost of data breach**

* Source: Mobile Security Index 2018, Verizon
** Source: 2017 Cost of Data Breach Study: Global Overview, Ponemon Institute, June 2017


$120B
spent on
IT security
Yet, 2/3 breached every year
Source: Gartner's Forecast: Information Security and Risk Management, Worldwide, 2017-2023

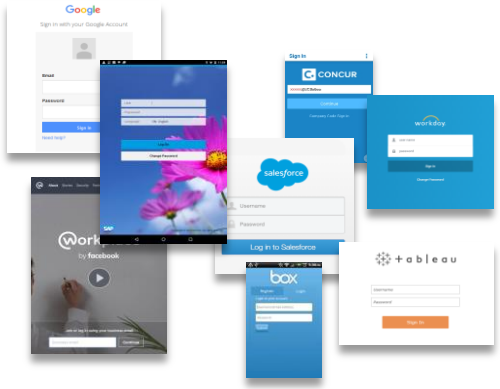
Passwords - top cause for data breaches

Not secure

81% of breaches involve weak, default or stolen passwords*

Not user-friendly

62% of respondents reported extreme user irritation with password lockouts**

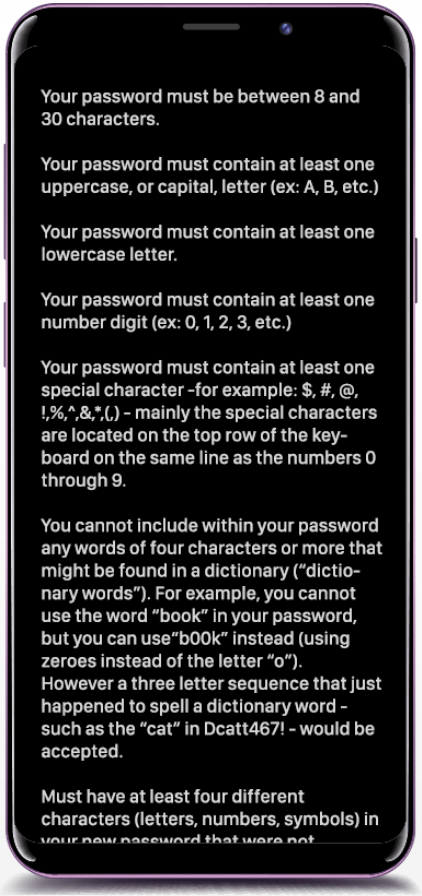


Not intelligent

Password based authentication lacks device, app, network, and threat context

* *Source: Mobile Security Index 2018, Verizon*
** *Source: Say Goodbye to Passwords, IDG Research, Jun 2019*

mobileiron



86%

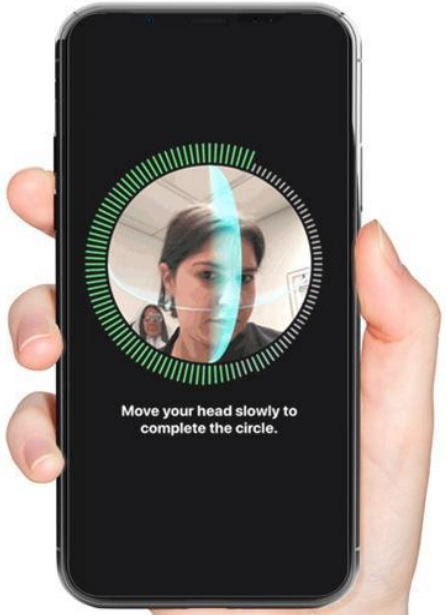
would do away with passwords if they could and believe they can reduce their risk of breach by half

Source: Say Goodbye to Passwords, IDG Research, Jun 2019

Zero sign-on experience

Mobile: More powerful than you think

Ever-present



Biometrics becoming your identity

Amazing consumer experiences

Zero sign-on for the knowledge worker

10:30 AM

Alice receives a new tablet.

She turns it on, enters her account information and the device is automatically provisioned with business apps and settings

She launches the Oultook app and gets access – **without a password**

6:00 PM

Alice is impressed by IT.

Down time. Alice downloads a fake version of Angry Birds from the app store on to her new tablet.

She gets a threat notification with instructions to delete the malicious app, while business apps, data, and connections from the device are suspended. After deleting the rogue app, business connectivity is restored.

4:00 PM

Alice is relieved and goes on to find the right version of Angry Birds.

After a day full of good meetings, Alice is back in her home office. She decides to update Salesforce on her personal desktop.

She is asked to scan a QRcode suing her MobileIron secured phone. After a quick biometric authentication, she gets secure access to Salesforce, on her personal desktop – without a password.

11:30 AM

Alice wants to submit travel expenses for a customer visit she made the previous day.

She launches the already provisioned Concur app and is given access – without a password

Alice continues to be impressed.

1:00 PM

While working in Salesforce,
Alice discovers a new app – Pulsar which allows offline access to Salesforce data

She attempts to connect Pulsar with Salesforce.

She is denied access and receives a custom notification to contact IT, who can onboard Pulsar as a secure app, if needed.

mobileiron

Zero sign-on for the knowledge worker

Requirements:
- Automated deployment
- Minimal user interaction
- Reliable enrolment process

Benefits:
- Easy device onboarding
- Increased productivity
- Passwords eliminated

Solution:
mobileiron UEM
mobileiron ACCESS

Requirements:
- Frictionless authentication
- Zero trust security

Benefits:
- Zero sign-on for password free user authentication
- Prevent unauthorized access

Solution:
mobileiron ACCESS

Requirements:
- Always-on mobile threat defence
- Automatic activation of threat defence
- Closed loop compliance and remediation

Solution:
mobileiron THREAT DEFENSE

Benefits:
- Real-time protection from mobile threats
- 100% adoption with minimal user impact

Requirements:
- Prevent unauthorized apps and clouds from accessing business data

Benefits:
- Stop data leaks to unauthorized clouds
- Maintain GDPR compliance
- Intuitive remediation for users

Solution:
mobileiron ACCESS

Requirements:
- Passwordless access on unmanaged devices
- Protect data on personal desktops

Benefits:
- No unauthorized access
- Secure access to business data from any device

Solution:
mobileiron ACCESS

mobileiron

Platform & product overview

Mobile-centric, zero trust platform for zero sign-on

1

mobileiron UEM

The foundation

Heterogeneous device management & security

Broad management use cases including frontline workers and contractors

Foundation for mobile-centric, zero trust security

2

mobileiron THREAT DEFENSE

The added layer of security

Fundamental to ensuring device (and ID) is secure

Data source for security analytics

3

mobileiron ACCESS

The authentication and access layer

Eliminate passwords with zero sign-on

Critical for future security architectures

mobileiron

Product capabilities

Zero sign-on

Biometric authentication on secure mobile devices

Passwordless access from both managed and unmanaged devices

Multi-factor authentication

Automatic MFA user enrollment

Mobile app push notification for easy identity verification

Zero trust policy engine

Adaptive authentication flows

Powered by UEM for device, app, and network signals

Protected by MTD against threats

Reporting

Detailed authentication logs

Visual dashboards based on user location, app type, and failure reasons

Standards-based

Secure cloud or on-premises apps including Office 365, Salesforce, G Suite, SAP, Oracle & so on

On any device including iOS, Android, Windows 10, and macOS

Integrates with IdP/ IAMs, SIEMs, and many more IT systems

Key takeaways

Benefits of zero sign-on

Better security

Reduce the risk of data breaches by eliminating passwords

Passwordless authentication from all devices - managed and unmanaged

Standards-based, zero trust conditional access for any cloud service or hybrid app

Frictionless user experience

Passwordless authentication to cloud services and hybrid apps

No more password resets or account lockouts also reduces helpdesk costs

Intuitive remediation workflows

No-win to win-win

Improve security hygiene by deploying solutions that users adopt

Gain confidence in driving innovation with mobile-cloud technologies

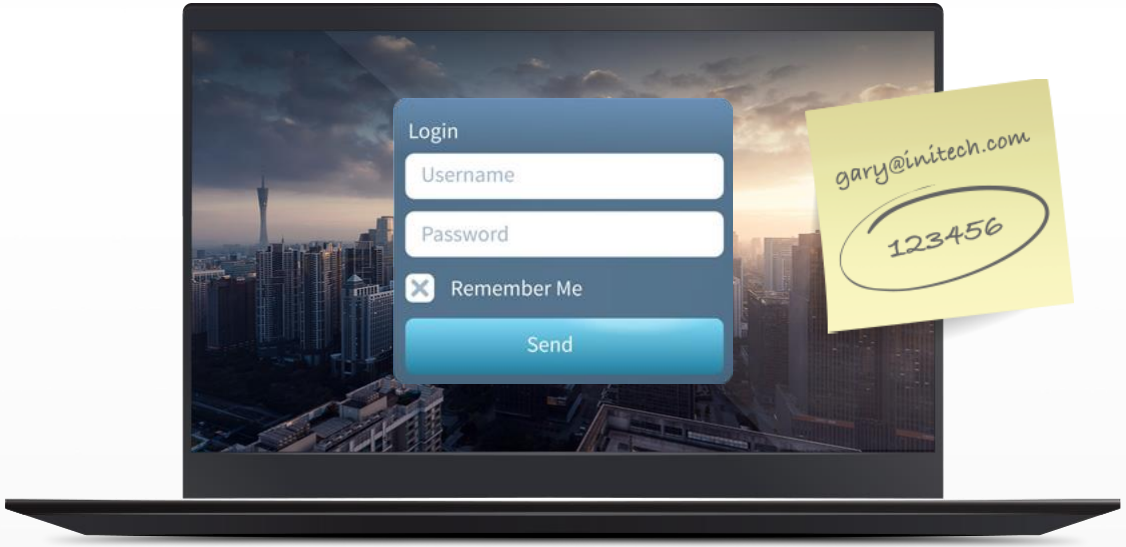
Optimize security spend and drive compliance

mobileiron

DEMO

mobileiron

The center of enterprise security



Passwords are a security risk

81% of breaches involve weak, default or stolen passwords

Source: Mobile Security Index 2018, Verizon

9/10

Security leaders believe that mobile devices will be your ID

IDG

Source: Say Goodbye to Passwords, IDG Research, Jun 2019