The Mobile Centric Zero Trust Approach

MobileIron Public Sector Team
Max Reitnauer
Max.reitnauer@ivanti.com
2407513295

Unmatched End-to-End Platform

Ivanti's Platform Enables IT Organizations to Discover, Manage, Secure, Service, and Automate Critical Workflows Across all Device Types

Discovery / Inventory

Client Management

Endpoint Management

EMM & MDM

Zero Touch Provisioning

Patch Management

Application Control

Zero Trust Security

ivanti

Service Management

Service Management

Experience Management

Zero Trust Network Access

VPN / NAC / Remote Access Control

Asset Management

Line of Business Management

Ivanti's Unmatched Three-Product Pillar

mobileiron

Leader in Federal and State compliance and certifications

FIPS VALIDATED 140-2

AICPA SERVICE ORGANIZATIONS SOC aicpa.org/soc Formerly SAS 70 Reports

FR FedRAMP

PCi DSS COMPLIANT

CRIMINAL JUSTICE INFORMATION SYSTEMS CJIS

Privacy Shield Framework

Common Criteria

DISA Defense Information Systems Agency Department of Defense

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

General Data Protection Regulation

NIAP

HIPAA COMPLIANT

CIS Center for Internet Security

U.S. SECURITIES AND EXCHANGE COMMISSION MCMXXXIV

mobileiron

The Zero Trust Model

Assume Security Threats are already in your Enterprise

No Inherited trust, always verify…

Validate the device

Establish user context

Check app authorization

Verify networks

Detect and remediate threats

On-going compliance enforcement

mobileiron

mobileiron
THREAT DEFENSE

Real-time, on-device protection against known and unknown threats

Capabilities

Threat detection with machine learning algorithms

Detailed threat intelligence

Advanced app analytics

Local threat remediation and user notification on-device

Support for iOS and Android

Benefits

Easy to gain 100% user adoption with 1 app and automatic deployment

Insightful with immediate and ongoing visibility and risky app analysis

On-device detection and remediation without Internet connectivity
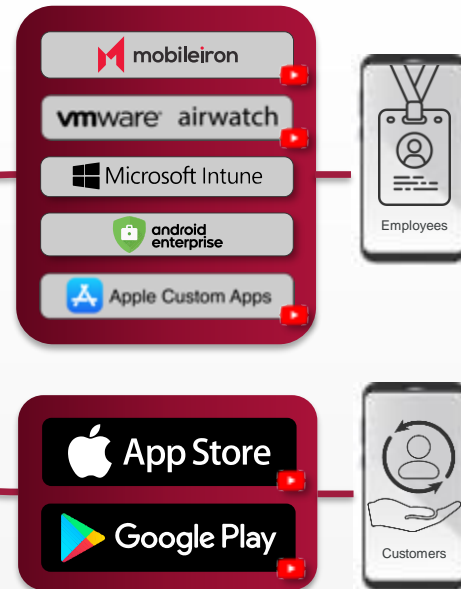
Attack use cases

Phishing

Network

Apps

Profiles

Advanced compromise

mobileiron

Challenges & Drag In App Publishing

CHALLENGES

- Business units develop more apps

- Push for more **frequent app releases** to deliver bugs fixes & feature updates faster

- **Long lead times** from development release to end-user availability

- **Unsecure data** in motion (app files) & data at rest (certificates)

- **Significant manual effort** for highly skilled IT specialists using a multitude of tools

- Prone to **human errors**, e.g. due to lots of copy/paste steps in the process

- Lack of app portfolio overview

- Many **stakeholders involved in release**, meta-data maintenance & localization

- **Endless emailing between business units, IT**, & external suppliers

- **Complex** and frequently changing mobile app **signing & resigning processes**

- **Lack of delegated administration** in **Apple and Google** tools

- **Sharing of certificates** causes **security and compliance issues**

- No audit trail for the app release process

Deploy App Updates

mobileiron
vmware airwatch
Microsoft Intune
android enterprise
Apple Custom Apps

Employees

App Store
Google Play

Customers

"Don't Give Up the Keys to the Castle"

mobileiron