Zero Sign-On Quick Reference Guide

Description

The ability to access enterprise resources from all devices, including devices not managed by MobileIron - without requiring passwords.Unlike single sign-on, which still requires a password, MobileIron enables password-less authentication by replacing passwords with mobile devices as user's ID. 81% of data breaches result from compromised credentials-Verizon DBIR; 86% of security leaders would do away with passwords, if they could-IDG,Jun19; 9/10 security leaders believe that mobile devices will be your ID-IDG,Jun1

User Persona	Buyer Persona	Executive Persona
Knowledge Worker	Security Buyer	CIO
Frontline Worker	Mobility Buyer	CISO

What Does It Do?

- Provide passwordless access to any business app or cloud service — including Microsoft Office 365 — through MobileIron's mobile-centric, zero trust framework
- Deliver a consumer-like authentication experience to the enterprise through the use of common biometrics
- Eliminate the hassle and security risks of passwords
- Ensure that only verified users, devices, apps, and networks can access business resources
- Provides in-depth reporting and alerting

What Are the Target Business Outcomes?

- Reduce the risk of data breaches from stolen credentials
- Provide frictionless access and eliminate the need to memorize, enter or reset complex passwords
- Reduce password-related help desk costs
- Deploy scalable mobile-cloud security on managed/unmanaged devices globally

Discovery Guidance	Discovery Questions
Risk mitigation strategy, helpdesk volumes, services/device/app infrastructure 1. Find the one Cloud service 2. Establish ROI 3. Validate viability of ZSO	• How do you reduce the risk of data breaches caused by stolen credentials? How are you managing passwords today? • How are your users authenticated? • How do you ensure universal, uniform MFA adoption? • How do you know authentication is from a trustworthy device or application? • How do new applications get onboarded at the LOB level? • How many helpdesk tickets are due to account lockouts?How many users fail phishing tests? • What Cloud services do you use? What IdP? Azure AD? • How do you prevent unmanaged devices, apps & services from connecting?

Competitors	Differentiators
MSFT, VMWare, Okta, Ping identity, Duo Security, Yubico, RSA	We truly eliminate the password. Our solution integrates with Okta (or other IdP/IAM) so you can continue using Okta for user management, account provisioning, privileged access management, while we provide passwordless user authentication and zero trust conditional access. We secure O365 and other SaaS apps, while eliminating the password. MSFT is primarily focused on securing O365 and does not eliminate passwords across all devices such as iOS and Android. Named a Strong Performer in The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019 report (MSFT & VMWare were NOT), plus highest scores for Device/ People/ Workforce Security & Zero Trust Roadmap & Differentiation.

Customer Case Study - Anonymous Global Enterprise Software Company

Challenges	Results
Secure access to 20 cloud apps and reduce security threats with a modern and secure authentication strategy.	• Reduce login time by 70%, saving 140 user hours/100K logins/month. • Reduce helpdesk troubleshooting time by 20% • Block unauthorized users and unmanaged apps