MobileIron | Mobile Device Management

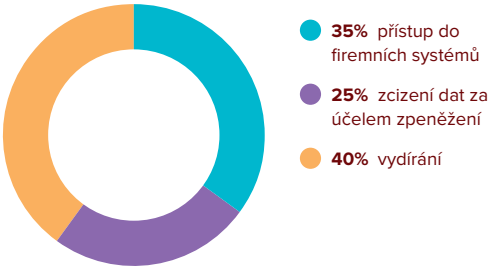
Úvod

V dnešních mobilních zařízeních je více osobních dat než v běžném PC. Proto jsou tato zařízení v poslední době ohrožena nejen ztrátou nebo odcizením, ale i čím dál častěji i sofistikovanějšími útoky, viry a malware, které mají za úkol převzít nad nimi kontrolu.

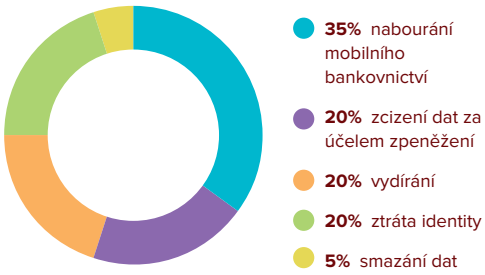
Počítače i notebooky mívají alespoň základní ochranu (automatické aktualizace operačního systému, aktualizované antiviry, zadávání hesla, certifikáty...). Naproti tomu mobilní zařízení (ať už chytré telefony nebo tablety) nemají často ani základní ochranu. Uživatelé většinou nemají ani nastavené přístupové heslo a už vůbec ne ochranu proti virům nebo dokonce šifrování obsahu.

Přitom obsah důvěrných dat na mobilním zařízení může velmi lehce vést k vytunelování bankovních účtů, ke zcizení diskrétního obsahu a následnému vydírání, prozrazení firemních smluv a jiných citlivých údajů, ukradení identity na sociálních sítích, e-mailech a podobně. To se netýká jen soukromých, ale zejména firemních mobilních zařízení.

FIRMY: Hrozby útoků na firemní mobilní zařízení
(procenta vyjadřuje míru pravděpodobnosti).



DOMÁCNOSTI: Hrozby útoků na mobilní zařízení
(procenta vyjadřuje míru pravděpodobnosti).



ZDROJ: APOGEO ESTEEM

Bezpečnost firemní infrastruktury

V mobilních zařízeních se čím dál častěji vedle sebe ocitají podniková i soukromá data. Na mobilní zařízení si uživatelé často bez rozmyslu přidávají neznámé a neověřené aplikace, které ve spojení s přístupem na internet, zejména v případě sociálních sítí, mohou šířit naprosto nekontrolovatelně informace i bez vědomí uživatele. Ti totiž velmi často nedbají na mobilní bezpečnost. Bezpečnost podnikových dat, a to i ukrytých za firemními firewally, je tak velmi vážně ohrožena.

IT manažeři náhle zjišťují, že ve firmách přestávají mít kontrolu nad tím, co se děje v jejich infrastruktuře a to právě díky mobilním zařízením. Ta svým principem fungování nabourávají i zabezpečené IT prostředí, přičemž uživatelé chtějí pracovat se soukromými zařízeními, která běžně připojují k podnikovým sítím (synchronizace pošty, využití WiFi ve firmě).

S novými mobilními zařízeními také ve firmách skončila jednolitost zavedeného operačního systému. Díky nim se ve firmách nyní vyskytuje třeba i pět rozdílných operačních systémů.

Jedním z komplexních nástrojů s možností správy, zajištění bezpečnosti a integrace mobilních zařízení do podnikového prostředí je MDM řešení od společnosti MobileIron.

Přednosti MDM

Mobile Device Management (MDM) od MobileIronu je komplexní řešení pro správu mobilních zařízení a na nich umístěných mobilních aplikací a firemních dokumentů.

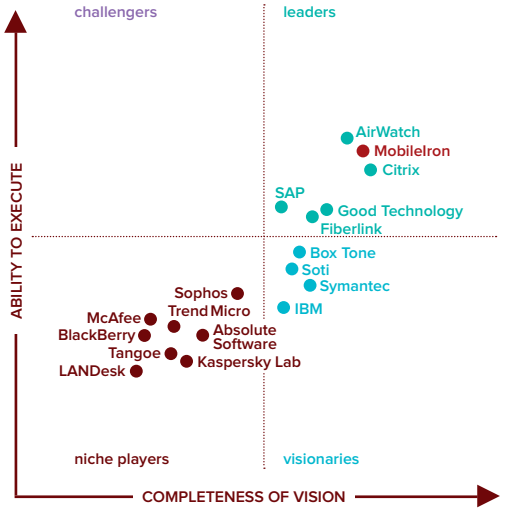
Pomocí MDM od MobileIron lze integrovat mobilní zařízení do firemní infrastruktury a určit, které aplikace a s jakým nastavením se do něho nainstalují a jaká forma zabezpečení zařízení, dokumentů i aplikací bude použita. Zaměstnanci mohou tedy efektivně pracovat i na svém soukromém mobilním zařízení a mít při tom bezpečný přístup do firemní sítě. Administrátoři IT mohou zase díky MDM jednoduše a efektivně ovládat celý životní cyklus mobilních zařízení od jeho registrace a nastavení, přes správu, až po jeho vyřazení z firemní sítě.

Centrální správa — MobileIron nabízí bezpečnou centrální bránu pro přístup mobilních zařízení z venku do firemní sítě. Pomocí systému MobileIron lze bezpečně spravovat nejen zařízení iOS, ale i jakékoliv zařízení se systémem Android či Windows Phone.

Šifrovaný oddělený kontejner — MobileIron díky AppConnect umísťuje firemní data a aplikace do separátního kontejneru v rámci mobilního zařízení. Každá aplikace tak dostane bezpečnou šifrovanou část a ona i její data jsou tak chráněna před neoprávněným přístupem z jiných aplikací nebo virů nainstalovaných na mobilním zařízeních. AppConect tak vytváří jakýsi obal kolem firemních dat a aplikací.

Bezpečný přístup k firemním datům — MobileIron využívá AppTunel, který je součástí AppConnect. Ten dokáže poskytnout bezpečný šifrovaný přístup k přesně specifikovaným zdrojům ve firmě bez nutnosti složitého sestavování VPN spojení, které běžně připojuje zařízení k vnitrofiremní síti zcela transparentně.

Testované aplikace — v rámci AppConect partnerství MobileIron testuje a certifikuje aplikace třetích stran, které musí splňovat náročné podmínky pro využití v AppConnect Ecosystému. Dostupnost bohatého „ekosystému“ bezpečných aplikací třetích stran je nezbytná pro úspěšnou podnikovou mobilitu.



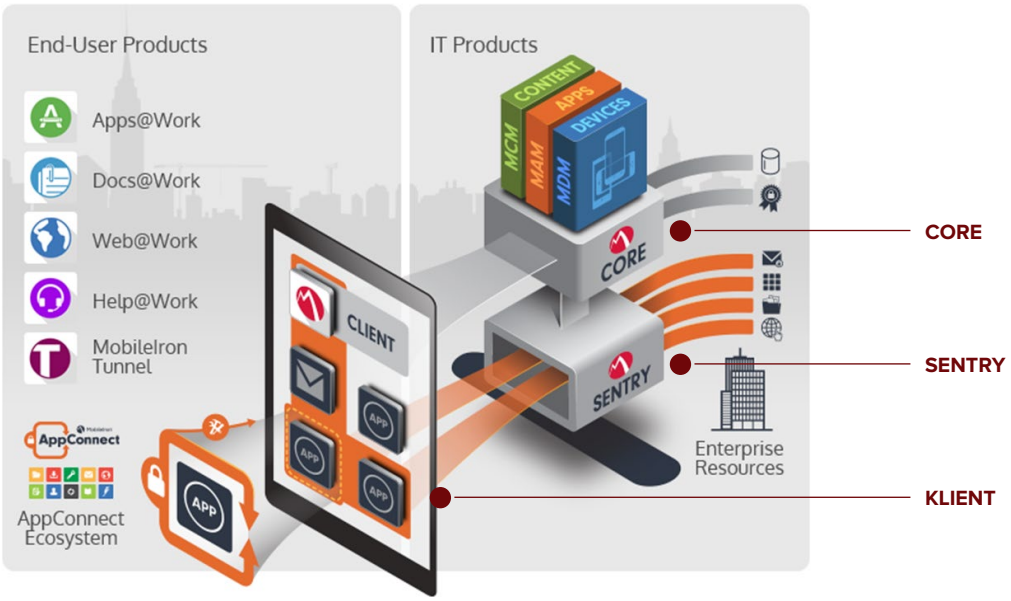
ZDROJ: GARTNER, INC., MAY 2013

Monitoring — SplunkForwarder a SplunkApp pro MobileIron umožňují sloučit všechny informace z MobileIronu s daty ze zbytku IT infrastruktury. Získávají kritické informace, podporují detekci hrozeb a pomáhají při řešení problémů. Software Splunk umožňuje získat více než 200 různých údajů z mobilních zařízení, které popisují stav mobilního prostředí firmy. Obsahuje reporting databázi, CSV export a dashboard s reporty pro názorný přehled získaných dat.

Možnost využití cloudu — MobileIron řešení lze využít i ve formě MobileIron Cloud, který se rychle přizpůsobuje požadavkům zákazníků s novými funkcemi a zákazník tak nemusí neustále řešit přechod na novější verzi. Cloud platforma je škálovatelná i na miliony zařízení.

MobileIron patří na špičku současného trendu ve správě mobilních zařízení.

Architektura řešení



Mobile Iron se skládá ze třech základních komponent:

① Core

Spojuje se s interními firemními servery a umožňuje administrátorovi IT definovat zabezpečení, spravovat politiky pro mobilní aplikace, pro obsah zařízení a pro vlastní zařízení (a to nezávisle na jeho operačním systému). Tuto část lze využít i ve verzi cloudových služeb firmy MobileIron.

② Sentry

Brána, která spravuje, šifruje a zajišťuje komunikaci mezi mobilními zařízeními a interními servery firemních IT systémů. Sentry vynucuje bezpečnostní politiky nastavené v Core. Zabraňuje prostřednictvím šifrování manipulaci s daty i jejich odposlech. Sentry může šifrovat e-mailové přílohy, které mají být doručeny na mobilní zařízení a které pak nelze otevřít jinou nepovolenou aplikací na mobilním zařízení a to ani při uložení do cloudu. Umožňuje směrovat požadavky pouze na schválené servery ve vnitrofiremním IT a odepřít přístup na nepovolené servery. Sentry je plně škálovatelná v clusteru i v rámci globálních organizací.

③ Klient

Třetí součástí je MobileIron klient, nazvaný **Mobile@Work**. Koncoví uživatelé si ho stáhnou z odkazu a ten automaticky nastaví přístroj tak, aby fungoval v souladu s firemním prostředím. Nastaví politiky, konfiguraci a zabezpečení stanovené IT oddělením. Zabezpečený MobileIron kontejner pak chrání podniková data a aplikace. Klient umožňuje nastavení e-mailu, WiFi, VPN a instalaci certifikátů. Oddělí firemní a soukromou část v mobilním zařízení. Klient umožňuje selektivně vymazat pouze firemní data na zařízení (např. pokud uživatel opustí společnost) nebo i kompletní smazání dat, když je zařízení ztraceno (ukradeno). Klient umožňuje automatickou instalaci podnikových aplikací. Klient umožňuje přístup k firemním datům za firewallem (např. k SharePointu).

Uživatelská část

Uživatelé v rámci klienta MobileIron mohou využívat (a administrátoři IT mohou nastavovat) následující funkce:

Apps@work

Slouží ke stažení a instalaci aplikací schválených a distribuovaných IT oddělením podle profilu uživatele.

Docs@work

Slouží k bezpečnému prohlížení, editaci a sdílení dokumentů mezi aplikacemi a umožňuje využití Data Leak Protection (DLP) na tyto dokumenty.

Web@work

Slouží k bezpečnému přístupu k webovým stránkám intranetu bez nutnosti sestavovat VPN spojení a to včetně využití DLP na tyto relace.

Help@work

Slouží ke vzdálené pomoci uživatelům zařízení od administrátorů IT.

DataView

Poskytuje monitorování využití mobilních dat. IT oddělení může nastavit limity přenosu a poté v reálném čase informovat uživatele.

Tunel

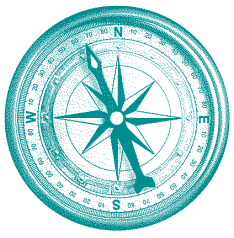
Umožňuje povolit konkrétní aplikace a zpřístupnit přesně specifikované zdroje za firewallem s tím, že neschválené aplikace a přístupy jsou blokovány.

AppConnect

Vytváří na mobilním zařízení zabezpečený kontejner, ve kterém jsou veškerá uložená data šifrována. Každá aplikace je v separátním kontejneru.

AppConnect Ecosystem

Schválené a certifikované aplikace třetích stran využívající technologii AppConnect.



ALEF NULA, a.s.
U Plynárny 1002/97, Praha 10
Česká republika
tel: +420 225 091 200
www.alef.com
cz-sales@alef.com

PRAGUE — BRATISLAVA — BUDAPEST

CISCO