Enterprise Mobility Management

Množství různých typů a celkové počty mobilních zařízení, pomocí kterých jsou dostupná firemní data, se neustále zvyšují.

To na jedné straně zvyšuje efektivitu práce zaměstnanců, ale na druhé klade nové nároky na správu a přináší nová rizika s mobilitou spojená.

Softwarové nástroje pro komplexní správu firemní mobility, tzv. Enterprise Mobility Management (EMM) systémy, přinášejí řešení, která umožňují spravovat a zabezpečit nejen samotná mobilní zařízení (MDM – Mobile Device Management), ale i aplikace (MAM – Mobile Application Management) a obsah přístupný na nich (MCM – Mobile Content Management) během celého životního cyklu zařízení.

Uživatelům tyto nástroje umožňují použití různých typů zařízení a operačních systémů při zajištění soukromí a intuitivního používání dané mobilní platformy.

Hlavní funkce a výhody EMM

Mobile Device Management – bezpečná správa mobilních zařízení s různými operačními Systémy přináší:

- zabezpečení přístupu k firemnímu emailu
- automatickou konfiguraci zařízení
- distribuci certifikátů
- selektivní mazání firemních dat ze zařízení vlastněných firmou i vlastněných uživateli
- kontrolu souladu s definovanou politikou

Mobile Application Management - kompletní správa životního cyklu firemních aplikací včetně:

- zpřístupnění aplikace ve firemním obchodě s aplikacemi
- zabezpečení aplikací na zařízení
- vynucení autentizace uživatelů
- oddělení firemních aplikací od soukromých
- odstranění zneplatněných aplikací

IXPERTA
Lihovarská 1060/12
190 00 Praha 9

IXPERTA HelpDesk 24/7
t: +420 242 492 222
e: helpdesk@ixperta.com

IXPERTA InfoLinka
t: +420 266 063 333
e: info@ixperta.com

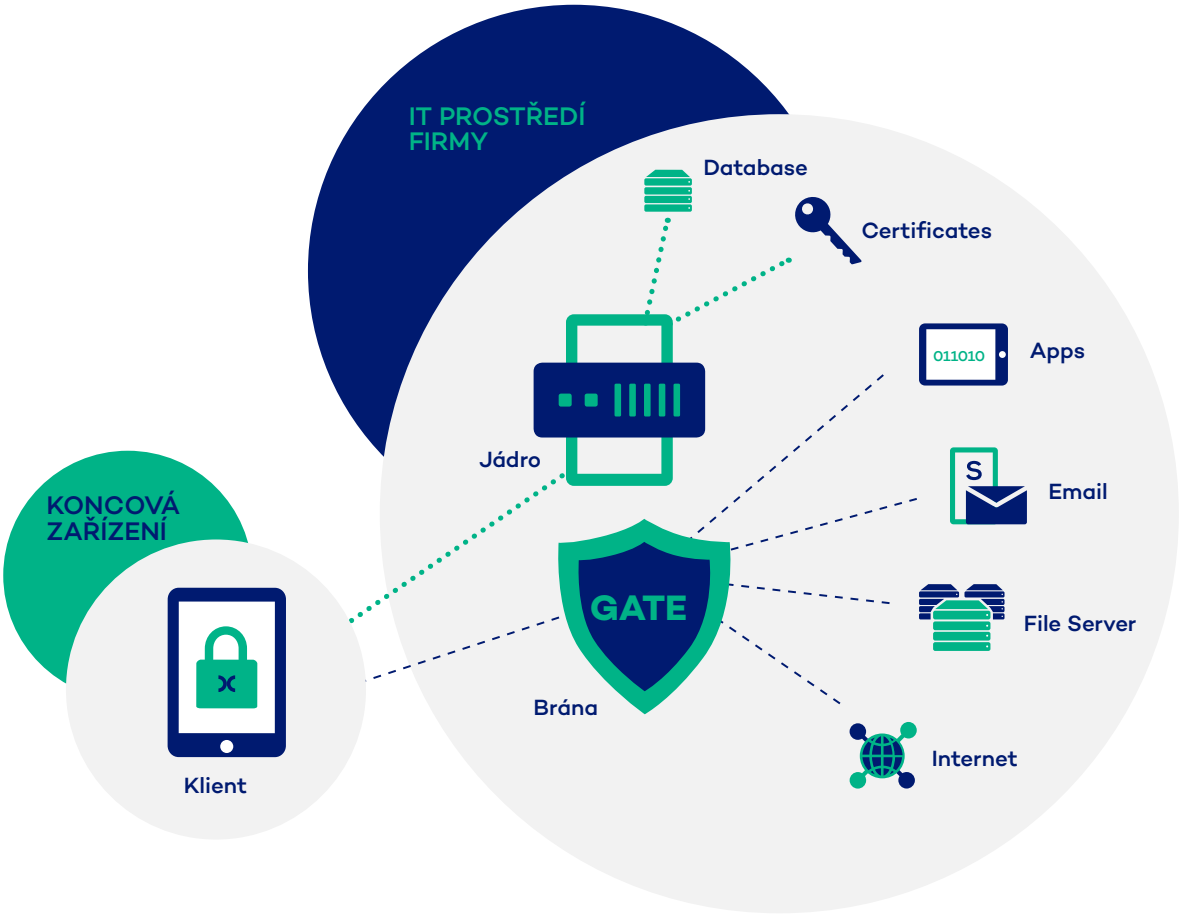
www.ixperta.com

IXPERTA

Mobile Content Management - zabezpečení přístupu k firemním dokumentům pomocí mobilní aplikace zahrnující:

- soubory na sdílených síťových úložištích
- soubory v systémech pro správu dokumentů
- přílohy v e-mailech

Architektura EMM řešení



JÁDRO představuje základní komponentu EMM řešení, která se integruje s back-endy firemních systémů jako jsou adresářové služby či dalšími systémy pomocí

IXPERTA
Lihovarská 1060/12
190 00 Praha 9

IXPERTA HelpDesk 24/7
t: +420 242 492 222
e: helpdesk@ixperta.com

IXPERTA InfoLinka
t: +420 266 063 333
e: info@ixperta.com

www.ixperta.com

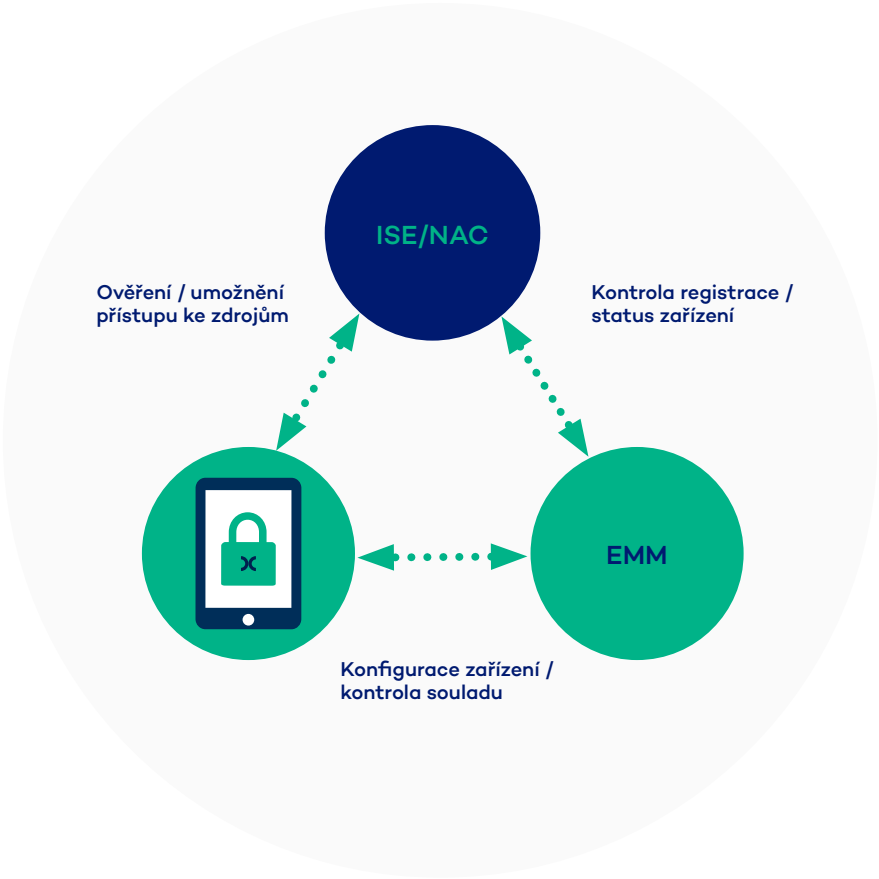
dostupných rozhraní API. Pomocí jádra jsou definovány politiky pro zařízení (MDM), aplikace (MAM) a obsah (MCM).

BRÁNA je klíčovou komponentou, přes kterou jsou přenášena data mezi back-end firemními systémy a mobilními zařízeními. Její hlavní funkce jsou správa, šifrování a zabezpečení přenášeného obsahu. Mezi nejzajímavější funkce patří např. vytvoření VPN tunelu podle požadavku konkrétní aplikace.

Na straně koncového zařízení je provozována klientská komponenta v podobě KLIENTA, který má za úkol automaticky zařízení nakonfigurovat takovým způsobem, aby odpovídalo firemních politikám. Pomocí klienta jsou uživatelům realizovány dále popsané funkce MDM, MAM, MCM.

Integrace EMM s dalšími firemními systémy

Enterprise Mobility Management řešení obsahují důležité informace o mobilních zařízeních a poskytují funkce, které mohou být ve spojení s dalšími systémy použity pro zvýšení zabezpečení firemních dat.



IXPERTA
Lihovarská 1060/12
190 00 Praha 9

IXPERTA HelpDesk 24/7
t: +420 242 492 222
e: helpdesk@ixperta.com

IXPERTA InfoLinka
t: +420 266 063 333
e: info@ixperta.com

www.ixperta.com

IXPERTA

Použití EMM společně se systémem přístupu do bezdrátové sítě (ISE/NAC)

V případě této integrace je připojení zařízení do firemní sítě podmíněno registrací do EMM a splnění souladu s definovanou politikou. V případě, že zařízení není do EMM registrováno nebo není v souladu s politikou, je webový prohlížeč uživatele přesměrován na registrační portál EMM, případně je zobrazen popis, co je třeba provést pro dosažení souladu. Po úspěšném ověření je zařízení/uživateli umožněn přístup k definovaným zdrojům ve firemní síti na základě politik systému přístupu do sítě.

Použití EMM společně s ochranou mobilních koncových zařízení

Systémy ochrany mobilních koncových zařízení poskytují další úroveň zabezpečení nad rámec běžných vlastností EMM. Tyto nástroje poskytují funkce, které chrání zařízení před hrozbami v operačním systému, v aplikacích i na síti. Dokáží je ochránit např. před zlomyslnými aplikacemi, nezabezpečenými Wi-Fi sítěmi nebo útoky typu man-in-the-middle. EMM je možné s výhodou použít pro automatickou aktivaci ochrany mobilních koncových zařízení v okamžiku zaregistrování koncového zařízení pod správu EMM.

MobileIron Check Point SOFTWARE TECHNOLOGIES LTD. CISCO Extreme Connect Beyond the Network Hewlett Packard Enterprise

IXPERTA
Lihovarská 1060/12
190 00 Praha 9

IXPERTA HelpDesk 24/7
t: +420 242 492 222
e: helpdesk@ixperta.com

IXPERTA InfoLinka
t: +420 266 063 333
e: info@ixperta.com

www.ixperta.com

Řešení infrastruktury – Enterprise Mobility Management od IXPERTA díky řešením Check Point

MTP

Mobile Threat Prevention

- Poskytuje nejlepší bezpečnostní řešení pro firmy, které potřebují řídit a zmírňovat rizika trendu BYOD a zároveň chtějí chránit svoje zaměstnance a firemní aktiva před hrozbami spojenými s mobilními zařízeními a internetem.
- Inovativní a pokročilé řešení pro firmy nabízí nejvyšší úroveň kontroly proti ohrožení při využití BYOD a je jediným řešením, které detekuje zařízení, aplikace a hrozby v celé síti.
- Uživatelé ocení snadné používání a okamžitou detekci a současně odstranění mobilních hrozeb. To jim umožňuje zůstat bezpečně připojeni kdykoliv a kdekoliv bez kompromisů.
- Mobile Threat Prevention poskytuje podnikům nejen nejkomplexnější mobilní bezpečnostní řešení pro zastavení mobilních hrozeb na všech iOS a Android řešeních, ale poskytuje i informace o hrozbách v reálném čase včetně možnosti rozšíření do stávající bezpečnostní a mobilní infrastruktury.

Capsule Docs

- Check Point Capsule Docs představuje komplexní řešení, které řeší bezpečnostní výzvy, kterým čelí firmy a organizace při zachování mobility zaměstnanců, zařízení i dat.
- S tímto integrovaným řešením můžete poskytnout bezproblémové zabezpečení pro ochranu podnikových dat před hrozbami, vytvořit bezpečné podnikatelské prostředí na mobilních zařízeních a zabezpečených obchodních dokumentech, zařízeních a sítích.

Capsule Workspace

- S Check Point Capsule Workspsace jste schopni řídit přístup k firemním emailům, dokumentům, interním adresářům a zdrojům v rámci bezpečného prostředí.
- Osobní data a aplikace jsou odděleny od obchodních dat, což umožňuje bezpečné používání firemních prostředků a zároveň dovoluje chránit osobní údaje a aplikace uživatelů.

IXPERTA
Lihovarská 1060/12
190 00 Praha 9

IXPERTA HelpDesk 24/7
t: +420 242 492 222
e: helpdesk@ixperta.com

IXPERTA InfoLinka
t: +420 266 063 333
e: info@ixperta.com

www.ixperta.com