Enterprise Mobility Management

The number of different types and also the total number of mobile devices that can be used to access corporate data are constantly increasing.

While on one hand this increases the employees' work efficiency, on the other hand it also places new demands on management and brings with it new risks that are associated with this mobility.

Software tools designated for the comprehensive management of enterprise mobility, i.e. the Enterprise Mobility Management (EMM) systems, deliver solutions that facilitate not only the actual management and the security of mobile devices (i.e. MDM - Mobile Device Management), but also applications (i.e. MAM - Mobile Application Management) and the content that is accessible on them (i.e. MCM - Mobile Content Management) throughout the entire life cycle of the equipment involved.

These tools allow their users to use various different types of devices and operating systems while ensuring both privacy and intuitive use of the specific mobile platform.

The main features and benefits of EMM

Mobile Device Management – safe management of mobile devices with different operating systems provides:

- secure access to corporate e-mail
- automatic configuration of devices
- distribution of certificates
- selective erasing of corporate data from devices that are owned by the company and also from those that are owned by their users
- checking compliance with defined policy

Mobile Application Management – comprehensive lifecycle management of business applications including:

- access to applications in the Corporate App Store
- security of the applications on the device
- enforced user authentication
- separation of corporate applications from private applications
- removal of applications that are no longer valid

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

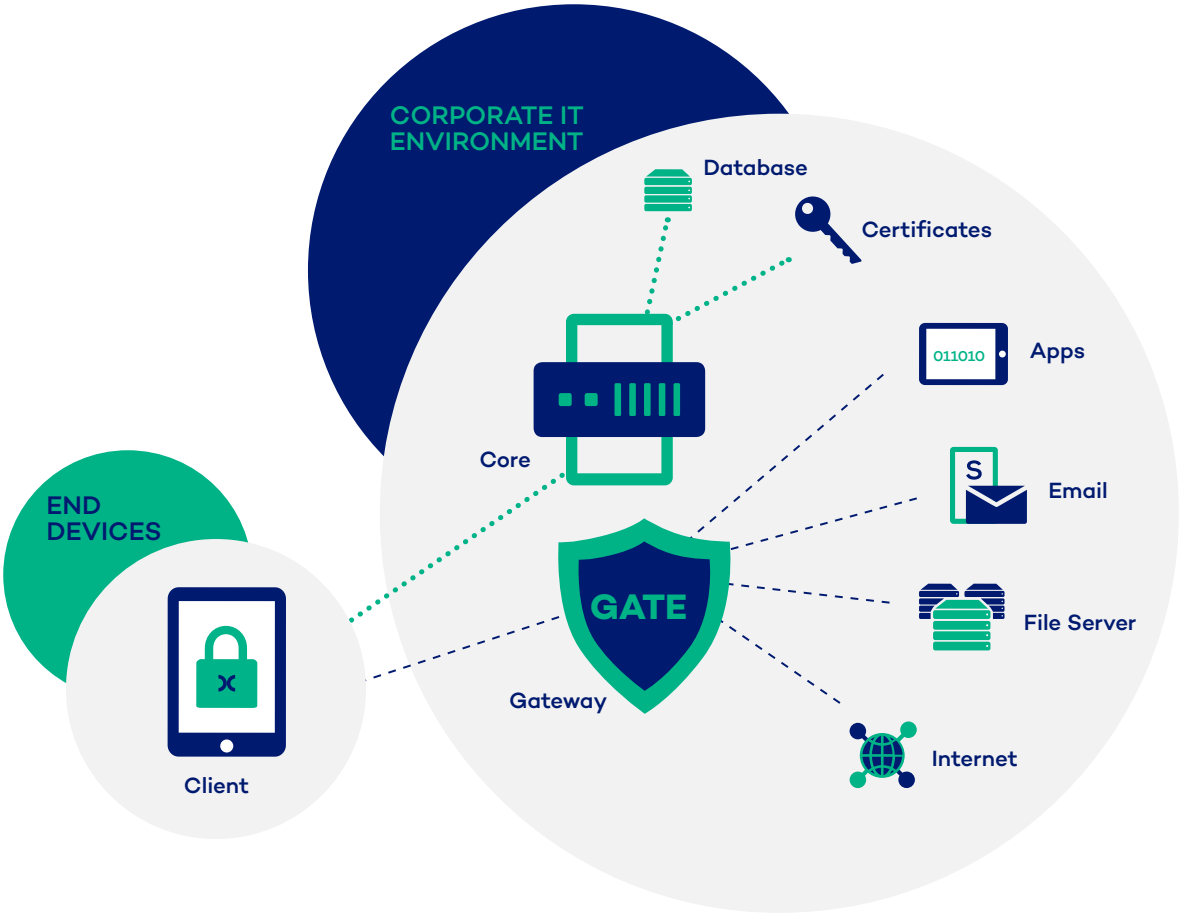
www.ixperta.com

IXPERTA

Mobile Content Management – enabling secure access to corporate documents via mobile applications comprising:

- files in shared network storage
- files in document management systems
- e-mail attachments

The architecture of the EMM solution



CORE is an essential component of the EMM solution that integrates with backends corporate systems as directory services and/or other systems that use the API's that are available. The core defined policies are the policies for device (MDM), application (MAM) and content (MCM).

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

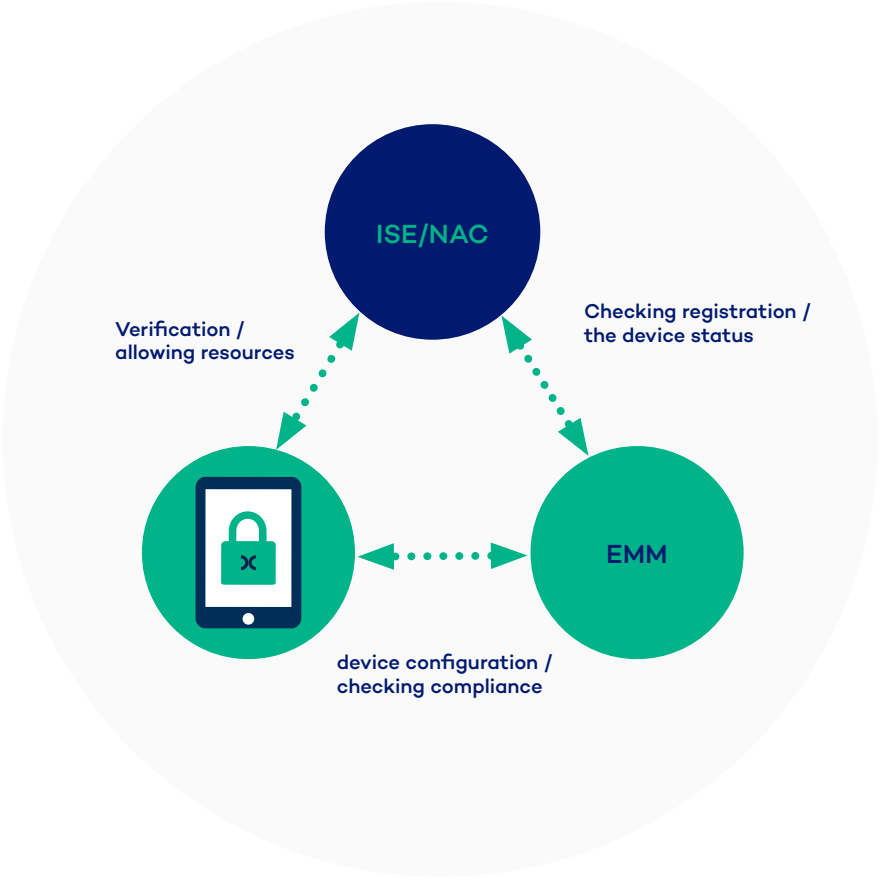
www.ixperta.com

GATEWAY is a key component, via which data are transmitted between the backend corporate systems and mobile devices. Its main functions include management, encryption and ensuring the security of the transmitted content. Its most interesting features include, for example, creating a VPN tunnel in accordance with the specific application requirement.

Operated at the device level is the client component, i.e. CLIENT, which is designated to automatically configure the device in such a manner that it matches the corporate policies. The MDM, MAM, MCM functions that are described below are provided for its users by means of CLIENT.

Integration of EMM with other corporate systems

Enterprise Mobility Management solutions contain important information about mobile devices and provide functions that, when combined with other systems, can be utilised for increasing security of corporate data.



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

Using EMM in combination with wireless network access system (ISE/NAC)

In the event of this integration the connection of the device to the corporate network is conditional on its registration to EMM and on compliance with the defined policy. If the device is not registered in the EMM or it is not in compliance with the policy, the user's web browser will be redirected to the EMM registration portal or a description of what needs to be done to achieve compliance will be displayed. After successful authentication, the device/user will be enabled to access the defined resources on the corporate network based on the access policies to the network.

Using EMM in combination with the protection of mobile end devices

Mobile endpoint protection systems provide an additional level of security beyond that of the typical EMM features. These tools provide a degree of functionality that protects against threats to operating system, applications and network. They can protect, for example, against malicious applications, unsecured Wi-Fi networks or attacks of the man-in-the-middle type. EMM can be used advantageously for automatic activation of the mobile endpoint protection from the time of the registration of the end device within 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

Infrastructure Solutions – Enterprise Mobility Management from IXPERTA using Check Point solutions

Mobile Threat Prevention

- This system provides the best security solution for those companies that need to manage and to mitigate risks associated with the BYOD trend and who also wish to protect both their employees and their corporate assets from threats that are associated with the utilisation of mobile devices and/or of the Internet.
- This innovative and advanced solution offers companies the highest degree of protection against threats associated with the use of BYOD and it is also the only solution that detects devices, applications and threats across the entire network.
- The users will appreciate the ease of its use and its instant detection and also the removal of mobile threats. These features will enable them to remain securely connected anytime and anywhere, without any compromise.
- Mobile Threat Prevention not only provides for companies the most comprehensive mobile security solution for blocking mobile threats to all iOS and Android solutions, but also provides information about potential threats in real time, including the possibility of an expansion to the existing security and mobile infrastructures.

Capsule Docs

- Check Point Capsule Docs represents a comprehensive solution that addresses the security challenges that are faced by businesses and by organisations, while at the same time also maintaining the mobility of their employees, their devices and their data.
- Using this integrated solution you can provide seamless security to ensure the protection of enterprise data from threats, for creating a safe business environment for mobile devices and for secured business documents, devices and networks.

Capsule Workspace

- With Check Point Capsule Workspace you will be able to manage access to corporate e-mails, documents, internal directories and other sources from within a secure environment.
- Personal data and applications are separated from corporate data, thereby enabling both the safe use of corporate resources and the protection of users' personal data and applications.

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