Communications Security Establishment Canada · Centre de la sécurité des télécommunications Canada

Mobile Device Management (MDM) Solutions
Guidance for the Government of Canada
ITSB-64

Introduction

Mobile devices have spread rapidly across the Government of Canada (GC) corporate enterprise and while they boost productivity and efficiency, they significantly increase the risk of a compromise to sensitive information. To help mitigate this threat, Communications Security Establishment Security Canada (CSEC) recommends departments utilize a Mobile Device Management (MDM) solution.

MDM software has the capability to secure, monitor, manage and support mobile devices deployed within a network by controlling and protecting data and configuration settings. However, the capability of different MDM software packages can vary greatly and care should be taken to select the appropriate solution.

What can an MDM do?

MDM solutions are available with a wide range of capabilities, ranging from the most basic solutions which control security settings implemented inside the mobile device, to more advanced solutions which extend and enforce corporate security policies and controls of mobile devices and provides seamless integration with corporate systems and services.

MDM products can provide one or more of the following functions:

1. **Management of Mobile Devices**

   - Provision devices – device settings, restrictions, credentials
   - Control devices – audit devices, password reset, remote wipe
   - Application Management – control what applications may or may not be loaded and used.

2. **Facilitate Securing of Corporate Data**

   - Data-in-Transit
   - Data-at-Rest

3. **Messaging/Email Integration**

   - Full integration and support for all major features (calendar, contacts, and support for all major platforms: Microsoft, IBM, GroupWise, etc.)

4. **Unified Communications Integration**

   - Support for all major platforms such as: Microsoft, IBM, Cisco, Avaya, Mitel, Siemens, etc.

5. **Enterprise Enablers**

   - Support, access and control for intranet and corporate web services and applications.

The extent of device settings and restrictions, and types of audit, control and application management available is usually dependent on the choice of mobile device platform, whereas support for the other functions is usually dependent on a combination of platform and MDM support.

More advanced MDM products work with the increased security and enterprise functionality built into the mobile device platform to extend corporate security policies and controls to the mobile device and to provide seamless integration with corporate systems and services.

A more limited number of MDM products also provide capability to:

Canada

Communications Security   Centre de la sécurité
Establishment Canada   des télécommunications Canada

- Secure corporate data that is stored on the device (data-at-rest); and

- Make secure connections to corporate infrastructure (data-in-transit).

Such mechanisms often rely on the use of an MDM agent (special application running on the mobile device) to implement these features. The effectiveness of such mechanisms tends to vary from mobile platform to mobile platform, and MDM vendor to MDM vendor.

MDM Limitations

An MDM solution must consider both the capabilities of the MDM product as well the choice of the mobile device platform(s), taking into account the capabilities and support for security features. The choice of an MDM should NOT be made independently of the choice of the mobile device.

Do not rely on the addition of an MDM solution to make up for poor mobile device security. MDM cannot add missing security features to a platform or device; it can only make use of the security features and controls that a mobile device platform supports natively.

Some MDMs can extend security features on a mobile platform, but require a software agent running on the platform. Such features are generally fairly limited and considered weaker and less robust than natively supported features.

Summary

When considering allowing the connection of mobile device platforms into the GC corporate enterprise, managers must realize that MDM solutions are not the silver bullet to solving the security issues brought by these platforms. They must consider both the limitations and capabilities of the MDM solution, and the choice of the mobile device platform and the device's set of implemented security controls.

Additional Information

For more information on IT Security advice, guidance and services, please consult CSEC's IT Security Client Services: itsclientservices@cse-cst.gc.ca.

Canada