Building a successful **Enterprise Mobility strategy**

MobileIron®

This white paper has been made possible by the sponsorship of MobileIron.

proximus

Enabling **the modern mobile enterprise**

Over the past decade, the rapid growth of worldwide mobility has been staggering. Since the arrival of the first iPhone in 2007, mobile devices have been spreading faster than any other technology in history. Mobile computing has changed everything.

Applications are no longer tied to the desktop and users expect to come and go seamlessly between desktops, tablets, and smartphones - anytime and anywhere. Today, the multichannel approach is evolving to an omnichannel experience and becoming the new normal for all consumers.

The Bring Your Own Device trend has taken root in organizations, as enterprises increasingly recognize its benefits by allowing employees to use their personal mobile devices for work-related purposes. Enterprises are going mobile, with or without the express consent – or even knowledge – of their executive bodies. In many cases, the mobility trend is driven from within the organization, as marketing departments, line of business managers and pioneering users accelerate the need for a mobile strategy.

Enterprise mobility concerns go beyond your own employees. Increasingly, customers – but also providers, subcontractors and other key stakeholders in your ecosystem – are using mobile devices to gather information about your company and products, to interface with sales and management personnel, and to purchase or provide products and services.

Efficient company operation requires IT organizations to accommodate mobile users while monitoring and managing usage to maintain safety and security. Companies need new strategies and technologies to confidently move forward on their mobile journey.

As you will discover from reading these pages, enterprise mobility is not just about buying the latest technology or putting email on an employee's phone. Mobility is about transforming your business to drive the emergence of new productivity sources. Proximus can help you build a sound enterprise mobility strategy and assist you in securely transforming your critical business processes with proven, industry-leading enterprise mobility solutions and professional services.

A comprehensive approach to **enterprise mobility**

EMM, the foundation of your enterprise mobility strategy.

If you are planning to manage anything on a mobile platform, Enterprise Mobility Management (EMM) is the starting point. EMM solutions connect mobile devices to enterprise workflows while supporting the continuous fluctuation in device numbers and types. Organizations use EMM systems and services to perform provisioning, tracking & auditing, support and data protection. EMM is the umbilical cord that links mobile devices to their enterprise infrastructure.

Three core EMM technical capabilities help IT organizations perform these services, some of which overlap. Organizations may use some or all of these resources, depending on their requirements.

1 Mobile Device Management (MDM)

Is an underlying technology that remotely manages the lifecycle of mobile devices and their respective platforms. MDM usually involves the installation of unique profiles on mobile devices, giving organizations the ability to remotely control, encrypt and enforce policies on smartphones and tablets. They can, for instance, be used to wipe a device of all apps and data if it is lost or stolen[1]. MDM also provides companies with real-time snapshots on device inventory, provisioning, or OS configuration, and can provide remote viewing and control tools for troubleshooting.

2 Mobile Application Management (MAM)

Tools allow organizations to manage mobile applications instead of hardware. MAM covers the deployment and updating of mobile apps, including administrative push support and app license management. MAM also enables organizations to apply security and control policies to these apps individually and selectively remove them – including associated data – from a specific device. Thus, corporate information can be protected without having to wipe a device entirely. MAM can also provide analytics capabilities to help administrators and application owners understand usage patterns.

[1] The National Belgium Rail, NMBS/SNCB, has reported a total of 17.589 lost mobile phones found in trains for the period 2011 to 2016

3 Mobile Content Management (MCM)

Enables professionals to access content on mobile devices. MCM has, according to Gartner[2], three fundamental roles. One of them is policy enforcement. Examples include conditional access to attachments in email, files synced with a back-end repository or files synced with a cloud repository. Another role of MCM is content push, which means that the MCM tool enforces rules for push-based file distribution, replacement and deletion. Integration is a further role devoted to Mobile Content Management: beyond basic file access policies, MCM tools are adding mobile compatibility for third-party rights management systems, as well as Enterprise Data Loss Protection (EDLP) and Enterprise Digital Rights Management (EDRM) solutions.

[2] Gartner, *Magic Quadrant for Enterprise Mobility Management Suites*, 6 June 2017

The expanding footprint of **Enterprise Mobility Management**

There are various vendor approaches to managing the mobile life cycle and the needs of organizations vary greatly across sectors, with most clients using MDM, MAM and MCM functionalities. Other features, such as Mobile Identity and Access Management (MIA), Mobile Information Management (MIM), Mobile Expense Management (MEM) and Containment, to name a few, are used by a smaller fraction.

Unified Endpoint Management (UEM)

Nevertheless, EMM is evolving beyond its original scope of mobile device, app, and content management, as client computing merges with mobile computing to form end-user computing groups. "The definition of EMM is evolving. EMM used to be mainly about mobile device and application management, but now it's more about enabling mobility more broadly – extending to Windows 10 and MacOS devices", says David Johnson, principal analyst at Forrester Research[3].

This has created the need for a single solution to manage both traditional client devices as well as mobile devices. Microsoft and Apple have added MDM APIs to their platforms to facilitate this convergence. The biggest challenge to implementing Unified Endpoint Management is that organizations usually have legacy requirements, such as complex Win32 applications and Windows GPOs that cannot currently be addressed with EMM tools. However, there are changes happening that will increasingly allow EMM tools to manage PCs. First, Microsoft continues to enhance the MDM APIs in Windows 10, closing the gap with GPOs. Second, EMM vendors are providing proprietary capabilities to address those gaps in areas such as security policy, managing scripts and deploying Win32 applications.

> "EMM is extending into unified endpoint management – combining EMM functions with PC and laptop client devices, from both a company-owned device and BYOD perspective. EMM platforms are also extending to non-traditional connected endpoints, such as wearables, digital signage, kiosks, and other IoT-related scenarios"[4].
>
> **Phil Hochmuth**, Enterprise Mobility Research program director at IDC

It should be noted, however, that not all IoT objects will fall under the scope of EMM tools. Some devices will be managed directly by manufacturers or will have proprietary management tools. And many devices will not need to be managed at all. In any event, it is clear that the diversity and number of devices will continue to grow, and IT organizations must be ready.

[3] Matt Kapko, What is EMM? Enterprise Mobility Management explained, Computerworld, 9 October 2017
[4] Phil Hochmuth, *IDC MarketScape: Worldwide Enterprise Mobility Management Software 2017 Vendor Assessment*, August 2017

Protecting your business **from mobile threats**

Policy enforcement will not be sufficient indefinitely as an answer to mobile security issues. By 2019, mobile malware will amount to one-third of total malware reported in standard tests, up sharply from the 7.5% spotted today, according to Dionisio Zumerle, research director for mobile security at Gartner[5].

Mobile Threat Protection (MTP)

Depending on industry, applicable regulations, data sensitivity, specific use cases and risk culture, organizations should seriously consider introducing Mobile Threat Protection solutions, gradually but without delay. Highly regulated bodies, such as financial institutions, and sensitive organizations, like healthcare facilities, would do well to adopt MTP solutions even sooner.

Although the mobile threat protection market is growing in terms of adoption, there is still a lot of confusion and uncertainty from end users regarding which risks MTP addresses and how urgent or useful MTP can be. Of course, using mobile threat detection and defense is no trivial undertaking: the technology must cover user, application, device (iOS as well as Android phones and tablets) and network-level threats to be effective.

MTP solutions should not only be able to detect anomalous behavior by tracking expected or acceptable behavioral patterns, it should also be able to inspect mobile devices for configuration weaknesses that could open doors to malware. MTP systems should be capable of monitoring network traffic, cutting off suspicious connections as well as scanning applications to identify those that could place enterprise data at risk.

And above all, IT organizations should pay special attention to selecting an MTP solution that optimally integrates with their EMM tooling.

Mobile malware has grown more than

100%

year over year in 2016, representing approximately

7.5%

of all malware

(source: AV-TEST T Security Report 2015/16)

[5] Gartner, *Market Guide for Mobile Threat Defense Solutions*, 22 August 2017

Proximus Enterprise Mobility Management

At Proximus, we consider EMM as the central integration point for mobile policies. Because it is the foundation stone for managing mobile resources at the enterprise level, **Proximus EMM** is the platform of choice for **federating policies for other services and tools**.

Thanks to its broad integration capabilities with third-party infrastructure components, our EMM solution provides a common, cross-platform baseline to set, contain, validate, enforce and update **device policies for an extensive range of tools and services**, such as gateways, proxies, VPNs, network access controls and certificates, application certificates, content and rights management systems, identity and access management, version controls and backups, system updates, or device initialization and wipe.

And as a single point of policy and accountability, Proximus EMM provides the opportunity to avoid agent inflation where a plethora of add-on utilities monopolizes local resources, complicating the task of policy coordination for system administrators.

Proximus EMM also includes an additional feature that provides conditional access to cloud repositories (MI Access). Unlike traditional security approaches, our solution correlates user identity with unique information feeds such as device posture and app state. Proximus EMM ensures that business data stays within IT bounds so it can't be stored on unsecured devices, connect to unmanaged apps, or share information with unsanctioned cloud services.

With our EMM solution, organizations benefit from a standards-based approach that can secure any cloud service, including Office 365, without requiring any proprietary integrations.

1 MDM component

The **MDM** component of our solution provides the foundation of any EMM solution by **allowing IT to enable employees to be productive on their preferred mobile devices and desktops**, secure and manage mobile devices and desktops across multiple operating systems (including Android, iOS, macOS, and Windows 10), provide secure corporate email, automatic device configuration, and certificate-based security. MDM allows administrators to selectively wipe enterprise data from mobile devices and desktops without impacting personal data.

2 MAM capabilities

MAM capabilities let IT **build and maintain an enterprise app storefront**, secure applications on any device, authenticate end users on the device, and separate business and personal apps on mobile devices and desktops.

3 MCM module

The **MCM** module enables IT to s**ecure corporate data on mobile devices and desktop**s without compromising the end-user experience. They provide an intuitive way to access, annotate, and share documents from email, SharePoint, and other enterprise content management systems as well as enterprise and personal cloud services.

Proximus EMM benefits all your company's stakeholders

Business benefits: security and compliance

- Helps bringing your organization into compliance with the EU General Data Protection Regulation (GDPR)
- Ensures no critical data gets in the wrong hands when a device is lost or stolen
- Ensures no data is leaked to third parties, intentionally or unintentionally
- Your employees have access only to data they are allowed to

IT staff benefits: control and ease of use

- Simple, secure management of the fleet of devices
- Efficient roll-out of preconfigured mobile devices
- Provides an overview of all mobile devices in your organization, where they are and who uses them
- Allows to enroll bulk users and mobile devices, and assign policies to them without having to do this individually for each device or user

Employee benefits: right balance between security, user experience and productivity

- Enables your employees to work from any location in a secure way

Proximus Unified Endpoint Management

While EMM already solves many of the most common use cases for PC management, until now there were a few gaps in the EMM model that prevented IT from moving away from traditional PC management tools.

Proximus UEM reconciles the mobile and desktop worlds. It extends EMM capabilities and offers a simplified way for IT teams to **modernize security and management for Windows 10** without sacrificing the granular policies and actions they have built up over the last 20 years.

Our UEM solution allows IT organizations to increasingly move away from a costly and confusing two-speed model where PCs are managed by traditional tools while mobile devices are managed by modern ones. Scripts that leverage GPOs can now coexist with EMM profiles, without the need for traditional PC management tools. All commands can now use the EMM protocol to send information to the device regardless of whether it is a script or an EMM API. This means that IT organizations can focus on increasing organizational productivity with greater efficiency and agility, and at lower cost – all without compromising device security for on-the-go users in the modern enterprise.

Benefits

Proximus UEM enables IT teams to:

- Have complete control over PCs with EMM
- Manage PCs remotely, over-the-air
- Reduce the need for imaging desktops
- Leverage GPOs-based commands with PowerShell scripts deployed by EMM
- Easily edit and manage Registry
- Effortlessly deploy non-MSI wrapped Win32 apps
- Gain File System visibility

Proximus UEM unlocks PC management capabilities not possible previously using EMM, such as:

- Defining a peripheral device
- Creating desktop shortcuts
- Determining the hardware connected to the device
- Having visibility into software on the device
- Understanding which files are in a folder
- Gaining visibility into the registry
- Making changes to the registry
- Removing useless or unwanted software from the device even if it is a system app

Proximus Mobile Threat Protection

While EMM solutions manage and enforce policies, they are not designed to specifically address the security posture of a mobile device, because they don't provide threat intelligence or detect malware.

Yet, mobile threats are on the rise and the amount of malware in app stores is increasing. The stakes are higher than ever:

> The average cost of a corporate data breach has been estimated at 18,000 € per day by the Ponemon Institute[6].

Proximus MTP uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning. Its dynamic threat response prevents compromised devices from accessing your organization's network, while allowing your organization to set adaptive policy controls.

Proximus MTP enables IT and security teams to:

- Perform advanced app analysis to detect known and unknown threats
- Monitor network activity for suspicious or malicious behavior
- Assess device-level (OS) vulnerabilities to reduce the attack surface
- Detect and block SMS phishing attacks designed to steal enterprise credentials

Proximus MTP never impacts device performance or battery life because the majority of its risk analysis is performed in the cloud. The on-device app runs seamlessly in the background until malicious activity is detected, alerting the end user to take action.

[6] Ponemon Institute, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, October 2016

Integrating with EMM

By integrating seamlessly with Proximus EMM – and with most of the EMM solutions on the market as well – Proximus MTP offers a comprehensive platform that adds a critical layer of security to Enterprise Mobility Management solutions. Our MTP solution can be used to dynamically change access privileges to reflect risk levels, transforming static management policies into active device protection.

Whatever the number of devices in your mobile fleet, integrating Proximus MTP with your EMM platform is fast and easy. Deployment and management can be done through your EMM automatically, accelerating adoption and reducing overall operational costs. Our solution scales with your EMM, seamlessly protecting enrolled mobile devices. As a result, you can rest assured you have the layers of security you need to both manage and protect mobile devices, even in a highly dynamic environment.

Benefits

- Deploy any iOS or Android mobile device on your organization's network with confidence
- Deploy any iOS or Android mobile device on your organization's network with confidence
- Protect sensitive information on mobile devices from espionage
- Improve visibility and protection against the latest mobile threats with mobile security that integrates easily into your existing mobility and security infrastructures (MDM, MAM, NAC, SIEM, etc.)
- Augment the security measures of Microsoft Exchange and container/ wrapper solutions
- Enable rapid response to cross-platform advanced persistent threat (APT) attacks
- Enable contractors to access corporate data safely from unmanaged devices
- Preserve user experience and privacy, while adding the protection required by organizational or regulatory mandates

Why choose **Proximus?**

Considering that **smartphone adoption is expected to grow from 1.47 billion devices in 2016 to more than 1.7 billion in 2021**[7], it is self-evident that organizations need to find a comprehensive way to quickly onboard and secure a vast range of employee devices coming into the enterprise.

With the combined strengths of best-of-breed technology providers – including **MobileIron** and **Check Point Software Technologies** – and the comprehensive professional services offerings of Proximus, organizations can achieve the benefits of mobile solutions that are truly business-class.

There is no one-size-fits-all approach to Enterprise Mobility Management, and many companies run into snags along the path to mobile enablement. Proximus can help you consider all the possible mobile scenarios, plan for the challenges, build a solid strategy, use the right technologies, set the appropriate policies, and leverage best practices to make a success of your mobile initiative.

The needs may vary significantly by size of company and type of activity or according to regulation conditions, and EMM requirements change as mobile platforms evolve. To keep abreast of these changes, engage Proximus experts to understand the changing mobile device landscape and the implications for mobility management.

Proximus offers the Enterprise Mobile Management Solutions needed by organizations to better serve their customers in today's digital world, along with the related technical consultancy services and managed services. Another goal of Proximus is to provide end-to-end services framed by clear SLAs.

Our Enterprise Mobile Management solutions enable you to:
- Avoid loss of critical data assets through robust EMM and MTP solutions
- Reduce complexity and drive down costs
- Simplify data management and daily operations
- Lower your IT footprint through highly-efficient resource utilization
- Understand how to mitigate risks, analyze return on investment to justify future investments
- Assess the current state of your business and develop a roadmap to support future initiatives
- Enhance service level agreements and improve the efficiency of your organization

We continuously work to improve our management systems by conducting reviews and audits. We also monitor and analyze our results and the feedback received from customers, employees, and other stakeholders in order to identify our quality, security, safety and environmental objectives and targets.

[7] IDC, *Worldwide Quarterly Mobile Phone Tracker*, 29 August 2017

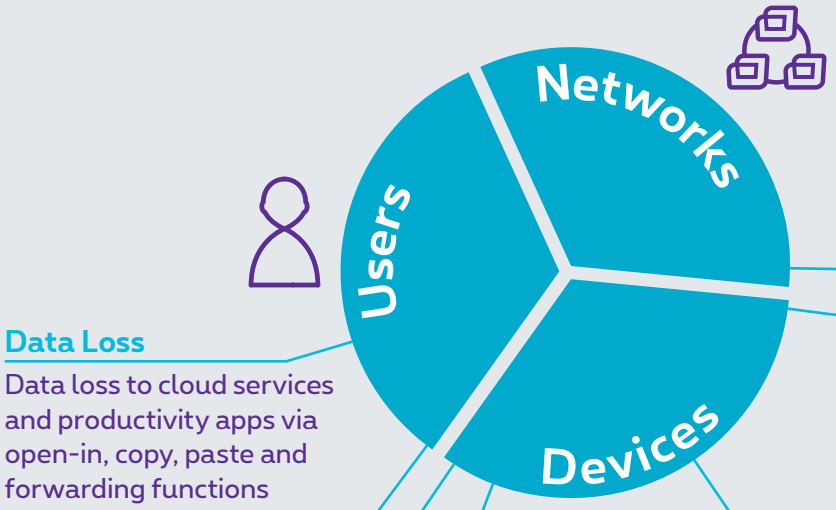
Facts and figures

Mobile threat vectors

One of the biggest mobile challenges IT must solve is securing data and apps – including third-party apps – on all mobile devices without impacting the native user experience. Before the mobile era, the biggest security risks were malware and viruses due to the vulnerability of open file systems and an unprotected kernel. Today, mobile operating systems have a sandboxed file system and protected kernel, so traditional security threats present less of a concern. However, mobile technologies face three other types of threats: user-based, device-based, and network-based.

Threat vectors on mobile are different from PC

Sandboxed mobile operating systems are secure. Threats, such as malware, are mitigated by OS design. Preventing data loss on mobile requires focus on a different set of risk vectors.



Always-On Connectivity
Mobile devices are hyper-connected and often access sensitive data over untrusted networks, increasing the risk of data loss through Wi-Fi sniffing, rouge access points and Man-in-the-Middle (MitM) attacks

Data Loss
Data loss to cloud services and productivity apps via open-in, copy, paste and forwarding functions

Device Tampering
Exploit OS vulnerabilities to jailbreak or root devices, bypass security, and install malicious apps from un-authorized app stores

Malicious or risky apps
Collect and share data such as personally identifiable information (PII) and device location with third party advertising and analytics system

Form factor
Portable form-factors make mobile devices susceptible to loss or theft

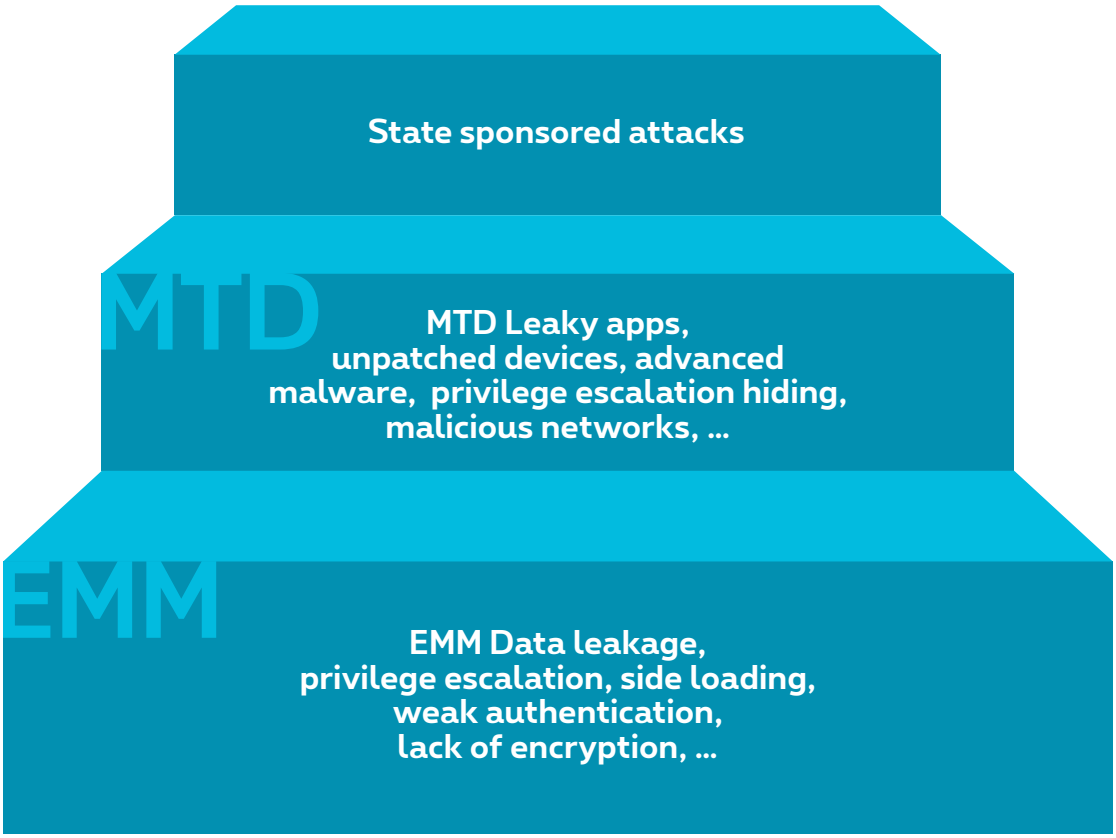
Source: MobileIron

Facts and figures

In March 2017, for the first time more Android than Windows simultaneous internet connections were observed

source: StatCounter, Android overtakes Windows for first time, 3 April 2017

Mobile security threats addressed by enterprise Mobility Management (EMM) and Mobile Threat Defense (MTD)



Source: Gartner, *Market Guide for mobile threat defense solutions*, 22 august 2017

More info

Proximus is your trusted mobile solutions advisor for the management of secure mobile applications, data, and services. Surf to **www.proximus.be/xxx** or contact your account manager.