Enterprise Mobility and the Digital Workplace, Increasing Smart Workers’ Productivity

In this Issue

- Summary: 2
- Market Challenges: 3
- Research From Gartner: Use Enterprise Mobility Management in New Ways to Optimize Mobile Investment and Reduce Unexpected Costs: 19
- About Telefonica Business Solutions: 24
Summary

The Digital Workplace is more than just a technological evolution of the traditional workplace: it’s a business strategy that more and more organizations are introducing in order to improve smart workers’ productivity. Enterprise mobility is a key lever for facilitating the Digital Workspace and making smart workers outperform. Mobile technology is changing the way we approach our work, it is making it easier to combine personal and professional life, and it is boosting employee productivity.

The Digital Workplace needs to cope with the consumerization of both human resources and technology evolving at an unprecedented breakneck pace. Employees feel more productive when they are able to use technology in the same way they use it in their personal life. This does not only mean the types of device they use, but also the set of increasing productivity, social, and cloud-based applications. These challenges need to be properly addressed by enterprises in a framework where corporate-owned devices live with personal devices in a Choose-your-own-device (CYOD) or Bring-your-own-device (BYOD) scenario. Smart workers need to be connected anytime and anywhere in a secure environment that permits a flexible and agile usage of their productivity applications. Enterprise mobility, properly addressed, offers a tremendous opportunity for organizations to tackle their digital transformation, particularly where the Digital Workplace is a key element.

This paper focuses on the Digital Workplace that runs under mobile operating systems (O.S). This means iOS, Android and Windows 10 that can be managed through enterprise mobility management software.
Market Challenges

Market transformation, globalization, and the digital era is generating new business models and new ways of increasing the productivity of smart workers.

Mobility is perhaps what has changed the way companies work the most, creating great opportunities but also bringing big challenges:

- The proliferation of mobile applications is allowing smart workers to perform any task anytime, anywhere.
- Mobility plays a predominant role in the digitization of an enterprises’ business processes and has expanded from an IT-centric approach to affecting every single unit in the organization. Digital Workplace initiatives are shifting to be even more smart worker centric.
- Mobility plays a key role in the relationship between companies and their customers and ecosystems, generating new business models and collaboration environments.
- Employees are increasing the use of their own device and applications to access corporate resources - known as Bring-Your-Own-Device (BYOD) or Bring-your-own-applications (BYOA). This creates more complexity around managing and defining security policies of IT departments to ensure that sensitive information is not compromised during theft or the loss of terminals, and to ensure the correct use of installed applications.
There are new devices with new operating systems, or operating systems with different versions that increase the complexity of their management and evolution: Smartphones, Tablets, 2 in 1, Wearables.

Finally, the use of these applications can increase the consumption of data across the devices and, consequently, the telecommunication costs. This creates a need for greater control of the data consumption.

Mobility has become the fundamental essence to increasing business productivity. Technology is moving very fast and continuous adaptation is paramount. This relentless innovation is what will continue to keep enterprises alive in a digital world.

As mentioned, Enterprise mobility plays an incredibly important role in this movement towards the Digital Workplace.

Figure 2 shows some of the main objectives for enterprises when adopting mobility and Digital Workplace strategies:

---

**Figure 1: Global mobility data**

- 7.3B Devices per person
- 1.4B Global population (estimated in 2016)
- 10B Global use of Internet from mobile device

- Half of the enterprise devices were mobile devices in 2015
- IBM Smartphones sold in 2016: Twice the number of PC’s
- 25% of companies will incorporate a corporate catalog of mobile applications in 2017
- 84% of companies, employees have access to the corporative data through their personal devices.
- In 2016, 38% of companies have a plan to stop supplying devices to employees.
  
  In 2017 more than half of the companies will require their employees to bring their own devices to work.

Source: Telefonica
The Digital Workplace journey

Within the Digital Workplace, different ‘Mobile Digital Employee Journeys’ can be generated depending on the sector, the customer or even in the customers’ ecosystem. This flexibility makes it possible to understand the benefits of the enterprise mobility and facilitate its integration into the company. Here is an example of a Mobile Digital Employee’s Journey during a typical working day.

1) Early in the morning, the employee reviews all annotations related to the work to be done during the day, as well as comments from collaborators through a social collaboration tool. All the information is in the cloud, so the employee and the team can access anytime, anywhere.

2) Once the employee is in a meeting with a customer, he can use all the information associated to the project (audio, video, plans, etc.) and he can electronically sign a document, (a contract or a NDA, for example). Data is automatically synchronized with corporate back-ends using secure VPNs.

3) On the way back to the office, he can report and submit expenses (taxi, lunch …). As soon as reports are fully approved, the rapid reimbursement system delivers the money back into the employee’s bank account. It reduces the administrative load of the company and increases the employee productivity by automating expense reporting tasks.
4) He can also establish an audio or videoconference with the team to share documents, assign tasks and responsibilities and the field force receives all task information previously assigned.

5) Every smart worker uses secure and managed services to ensure full integrity and secure access and to avoid threats and malware and applying remediation.

6) Throughout the day, the company can control the employee corporate expenses.

7) Even in BYOD scenarios, with an efficient management of personal and corporate environments the employee can use the same device for corporate and personal tasks. This provides him with a perfect balance between personal and professional life whilst guaranteeing total privacy of his personal data.

Source: Telefonica
The Digital Workplace benefits

The Digital Workplace is a key enabler in any digital transformation strategy. It provides ubiquitous access to business tools, balancing personal and professional life, and encompassing a smooth transition in the enterprises’ adoption of new generations of digital workers whilst retaining top talent.

Having a holistic approach to the Digital Workplace brings a number of benefits to enterprises:

- **Revenue growth**

  The Digital Workplace has a direct impact on revenue growth in different ways. Sales people’s work pattern changes dramatically, gaining more time for focusing on customers, generating new funnels and improving conversion rates. Accessing customer information, status, anywhere anytime is key. Geographical monitoring apps and analytics also contribute to optimize sales activities.

- **Measurable impact of digital transformation and increase in productivity**

  The Digital Workplace must be managed as a single entity including all apps, management tools, and support services for the end and authorized users. This approach brings a set of KPIs and SLAs that generates a digital dashboard with the overall impact of the Digital Workplace in each part of the organization.

- **Cost savings**

  Mobility as a service and employee profiling optimize the overall cost of ownership when adopting the Digital Workplace. OPEX based solutions or pay-as-you-grow models minimize initial investment and permit a progressive roll-out of digital strategies which, in turn, optimizes costs. BYOD scenarios provide significant savings in device acquisition. For corporate liable devices new OPEX models such as leasing that includes insurance, depot repair, and recycling, facilitate its adoption as an integrated part of the Digital Workplace. There is also a considerable cost saving by using mobile devices as a substitute for fixed phones, including softphones. Telecom expense management tools play a key role to optimize profiles versus real usage and making employees aware of real costs in different scenarios. Additionally, unifying the management of the Digital Workplaces brings automatic synergies and savings on resource allocation. This holistic approach generates a single supplier negotiation for the Digital Workplace that optimizes costs versus the traditional negotiations and management of each of the elements of the service with no control of the overall impact on the organization.

- **Collaboration culture boosts**

  Accessing all of the collaboration tools at a single glance, and providing a single access to them, naturally boosts productivity. This approach includes combining personal communication and social apps with others provided by the enterprise. Organizations need a degree of flexibility to avoid imposing the culture upon their employees, but to provide the means for an optimal collaboration in different areas or different geographies whilst always guaranteeing the security of corporate information. Along with audio, video or web conferencing, social network tools applied to organizations are also playing a progressive role in boosting collaboration.
The following table demonstrates the benefits of the Digital Workplace in different areas of the organization.

<table>
<thead>
<tr>
<th>Area</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchasing Department</td>
<td>Cost reduction maintaining the SLAs</td>
</tr>
<tr>
<td>CEO</td>
<td>Digital Transformation Strategy New Business Models No investments on non-core assets Increase employee productivity</td>
</tr>
<tr>
<td>CTO / CIO / Facilities Management</td>
<td>Securing access to information Cost savings and efficiency improvements Legal compliance Business continuity</td>
</tr>
<tr>
<td>Business Units / Strategy</td>
<td>New revenue engines Business process mobilization to increase sales</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Increase employee productivity Improve collaborative culture in the organizations Personal and professional life balance Retain talent HHRR processes digitization</td>
</tr>
<tr>
<td>Operational Units</td>
<td>Contribute to revenue growth Improve efficiency in the workplace</td>
</tr>
</tbody>
</table>

**The Digital Workplace at a glance**

The Digital Workplace allows employees to access business tools from their mobile device (smartphone and detachable) with a single click. These functions all have specialized support, service management and a specific web portal for provisioning, incident and reporting activities.

Through the Digital Workplace, employees can work anytime, anywhere with complete access to business processes and by using the best device for each task. It enables new, more effective ways of working, coping with the security challenges and controlling the costs.

Businesses can keep smart workers engaged by adopting on-demand environments that support top talented and use their own device, as the service allows BYOD scenarios.

The Digital Workplace is composed of five elements:

- **Devices.** Employees need the flexibility to choose the most effective way in which to access business applications wherever they are working from. Smartphones and detachables offer a complete set of capabilities to access the business. Value added services over the devices such as insurance, depot or recycling are also required.

- **Communications.** Strong connectivity remains a crucial requirement in the Digital Workplace, both at home, at the office and on the road; it is fundamental to ensuring that the communication technologies and business and collaboration applications are constantly available in order to drive business functions effectively. Voice and data communication through LTE is a must when on the move.
Business applications. Giving employees seamless access to business applications regardless of location is vital. Such applications also help virtual teams work cohesively and interact effectively, giving them instant access to the critical information they need. Security is key when accessing the corporate environment therefore any app and access to the corporation must be completely secure. Business apps are also a key enabler of the business as they can optimize customer engagement and the relationship with the organization’s ecosystem.

Full management and support: The management layer is a key ingredient to the successful implementation of a Digital Workplace strategy. Without an integrated management layer Digital Workplace pieces are treated separately which makes it very difficult to track the impact on the organizations and, in some case, could even have a negative effect. Management layers include end-user and authorized-user support, remote monitoring and diagnosis tools, service portals, and service management.

The business model is simple and based on a monthly fee, providing a predictable cost and allowing the evolution of the service if the
customer’s requirements changes or evolves. The flexibility offered by the Digital Workplace is based on its adaptability to both the company and the employee needs. The Digital Workplace revolves around employees’ needs—where enterprises can choose the technology tools needed for their employees to work effortlessly with optimized profiling.

**Customer experience in the Digital Workplace**

The main challenges a Digital Workplace presents from a customer experience perspective are the following:

- **Enabling a seamless provisioning of the Digital Workplace.** When provisioning means asynchronous activation of multiple apps of different natures, the end user experience can be impacted. This is certainly true for BYOD models or when no previous kitting or remote kiosk mode has been carried out. The questions here are related to how identity management can be unified in order to simplify the access to the workspace environment and applications with a single user/password or equivalent authentication mechanism (e.g. Mobile Connect). Additionally, applications must be active for a particular end-user when they are deployed to the device, and access to them must be synchronized within this deployment. A typically bad experience use-case, for example, is when the end-user receives the credentials before the app has been deployed on their device.

- **Ensuring the same experience across different devices.** Consumers are generally used to running the same app on different devices and demanding the same user experience regardless. This also applies to the Digital Workplace. Independently of whether the employee is accessing from a detachable Windows 10 device or switching to an iPhone, their experience and the managed data should be the same. Additionally, corporate and personal productivity apps must coexist. Virtual apps must be available through mobile devices in the same way they are available across the legacy Windows systems.

- **Maintaining visibility and control for the company’s authorized and end-users.** Providing systems for employees whilst having complete visibility and control of the process is paramount. Incident management is optimized as smart workers are perfectly aware of the status of the provisioning or updating which creates less frustration. At the same time, admin users have a holistic view of the status of the service at different levels (by app, by employee, by profile, by legal entity, by geography) which provides, together with the proper analytics and integrated dashboards, proactive monitoring of the status of the Digital Workspace as well as integrated measurements of the SLAs in place.

- **Providing end-user support.** Mobile interactive customer support tools and remote monitoring of the device are the two elements that should complete the optimal customer experience. Smart workers should be able to dynamically interact with a single point of contact for customer support to address any problem related to the Digital Workplace. Basic communication should be through a mobile chat and evolving towards video and digital assistants through machine learning. Remote monitoring tools must cope with the different O.S permitting remote agents to do proper troubleshooting over end-user device configuration or apps.
Digital Workplace components

Devices and connectivity in the Digital Workplace

There are three main challenges surrounding the increase of mobility adoption within organizations (see Figure 5).

These three barriers open a new scenario: mobility evolving towards ‘Mobility as a Service’ (MaaS). MaaS establishes the functional and operative framework which allows access to any resource associated to enterprise mobility, through a single recurrent fee. Devices and connectivity are the base and digital value-added services and e2e management are the key components for the differential value proposition.

Smartphones and 2 in 1 (detachable) devices appear as a key component in transforming the Digital Workplace with mobility. Detachables is a new device category which combines a tablet with LTE connectivity and a keyboard to work with mobility. This device can totally replace the fixed Mobility adoption challenges workplace.

---

**Figure 5: Mobility adoption challenges**

- **High cost:** To equip all employees with smartphones and potential to lose control over communications cost.
- **OpEx vs CapEx:** Eliminate high investment by using set monthly fees and a model that guarantees repurchasing. BYOD scenarios to eliminate device cost and ensuring that the company pays only for the corporate apps and traffic.
- **High administrative load:** due to apps and device management.
- **Decrease the administrative load** by e2e management, device refresh and insurance.
- **Tailor-made value proposition** for any customer in their enterprise mobility strategy.
- **Flexibility,** offering best-in-class products with an employee focus. Roadmap built according to specific customer needs.

_Source: Telefonica_
**Mobile communication plans** evolve in this new Digital Workplace scenario with unlimited voice and SMS, but limited LTE data depending on the contract and with a single, recurrent fee that varies depending upon the included data allowance.

This example illustrates three MaaS models related to the device:

**Option 1: Device purchasing**

This model includes devices (smartphones and detachables) to be bought through CAPEX or through a Financial model. There is a possibility to repurchase the old devices and to offer access to an indoor coverage facility for free or for a reduced price.

**Option 2: Operative leasing**

A lease is a contractual arrangement calling for the lessee (user) to pay the lessor (owner) for use of an asset. In this case the assets are the devices. Operative Leasing drives a reduction on the monthly fee through advancing the residual value of the devices. The devices don’t belong to the customer and at the end of the lease, the customer must give them back.

This model includes devices (smartphones and detachables), and mobile insurance (by default) offering the turnkey product to B2B market (renting devices + delivery logistic + post sale), helping to reduce complex acquisitions costs and budget obstacles whilst allowing the benefits of renewals and out-of-date technology.

---

**Figure 6: An example of the MaaS model**

Source: Telefonica
At the end of the contract, Telefonica collects back all devices and offers new device rental (upgrading) with the latest technology and a competitive monthly price.

**Option 3: Split Billing-BYOD**

Split billing is a new generation cloud service, highly secure which allows multiple numbers (MSISDNs) to be associated to a unique SIM card: Two numbers and two active plans in one unique mobile device and the bills are completely isolated.

The split is across Voice, SMS and Data and allows enterprises to offer BYOD (Bring Your Own Device), where the personal device is used for business tasks.

With the ability to offer BYOD feature integrated in the enterprise’s digital plans, the customer receives a simple and flexible offer and a way of controlling the costs. Not only is there cost saving around the device provision, there is also a decrease in administrative tasks as the bills are split automatically. It opens the possibility of increasing the number of employees in mobility, accessing the business anytime, anywhere with the same underlying cost of ownership.

The market is now ready for this BYOD trend.

---

**Figure 7: Telefonica market analysis in Chile, Mexico and Argentina**

- **50%** More than 50% of companies refunded employee expenditure (partially or totally)
- **86%** Would your company employ an economic communication plan for employees to use their mobile devices with the company paying only for the business comms?
- **14%** Lines increase
- **90%** Companies will increase enterprise mobility up to 30% for voice, SMS and data.
- **89%** (Current enterprise mobility penetration 15%)

Source: Telefonica
Management in the Digital Workplace

Due to the variety of components of the Digital Workplace, a number of service management capabilities are required to properly address the challenges involved. This includes both end-user and authorized-user support, remote monitoring and diagnosis tools, service portals, and service management. Additionally, in some big corporations, multinationals or public administrations, additional professional services could be required related to IT integration.

This management layer is a key ingredient to success when implementing a Digital Workplace strategy. Without an integrated management layer Digital Workplace components are treated separately which makes it very difficult to track the impact on the enterprise and, in some case, could even have a negative effect.

An integrated management service provides full visibility and control and help to properly measure the huge benefits of adopting a Digital Workplace strategy.

Service Portal

The service portal in the Digital Workplace provides the proper tools for authorized and end users to manage the service. For end-users it grants access to the portals related to the different apps when non mobile access is required, or additional features not included in the mobile version of the app are needed.

For authorized users, it provides the system support for an integrated management of users and all of the components of the service. It also includes a dashboard connected to analytical tools, providing enhanced information and reporting of the status and evolution of the service, including SLAs. Through the portal, the authorized-user can track the status of orders, raise incidents and track their resolution status, and manage all of the components of the service. Having a service portal for managing the Digital Workplace as a single entity generates many synergies due to a unified management with all the components of the service, even at a vendor level. The complexity of dealing with multiple vendors, different tools and different support channels is removed, which automatically creates cost savings and efficiencies. It also provides better analytics with tools that provide insights around the impact on the business and the digital transformation status of the organization as a whole.

The service portal requires flexibility for profile definition across large organizations, and even support of different app types depending upon the organization’s specific needs - for example, internal native apps.

End-user support

In the Digital Workplace end-user support is mandatory in order to provide the best experience. End-user support must go beyond traditional troubleshooting and incident management, to include advisory services on how to use the different productivity apps. The relationship with end-users must be as interactive as possible. Normally, the preferred channel is the chat function. We see the evolution of video chat as a trend in the coming years, supported by machine learning and artificial intelligence. This support could be part of the IT service organizations’ offer to employees but in the Digital Workplace, due to the complexity of elements included, there is a clear trend to include it as part of the solution of the selected provider. This support must be flexible to cope with all the Digital Workplace elements, including standard third party apps, but also internal apps developed by the organization itself.
Authorized user support

Authorized users need dedicated support to deal with the Digital Workplace lifecycle. Typically, this includes specialized support for the ordering process (provisioning, activating, user management), incident management, change management, and report management. This support is more similar to the traditional 24x7 support an outsourcer can provide, but in the same way as the end-user support mentioned previously, authorized users can also enter the mobile arena with mobile chat, and so on.

Telecom Expense Management (TEM)

Telecom Expense Management is even more relevant in these types of scenarios because it helps to optimize worker profiling and adapt service cost to the real usage of services. Additionally, in BYOD scenarios it is critical to split professional and personal information integrated in the TEM and service portals. In the Digital Workplace TEM evolves not only to control mobile or fixed assets, but also to provide license management for cloud and mobile apps in order to have a complete inventory and control of the total cost of ownership. The connection of TEM tools with analytics and big data techniques provides a deeper understanding not only of the expenses (predictable expense management) but also on how the internal and external relationships in the organization are flowing.

Security in the Digital Workplace

Today, security around mobile devices is one of the key concerns for any enterprise across any industry, especially when adopting a BYOD model. A mobile-first strategy prioritizes mobility as the Digital Workplace versus the traditional environments. BYOD implies open corporate access to devices that are not fully controlled by the enterprise.

Both strategies have clear advantages that range from cost reduction to a significant productivity increase, mobilizing business processes and working anywhere, anytime. But a controlled, managed, and secure framework is needed in order to minimize the inherent risks linked to data loss, or compromised devices that could affect critical data held on the device or in the internal corporate networks.

Enterprise mobility management systems, thus Mobile Device (MDM), application (MAM), and content management, together with mobile threat protection tools tackle this problem by providing the proper tools to secure the Digital Workplace. Taking into account the level of complexity that mobility brings to any enterprise, dealing with different device manufacturers, different O.S that change frequently and different locations with connectivity provided by different mobile network operators, MDM offers the proper tools for a simple management and centralized control across devices. MDM deploys security policies for devices, apps, and content, including public SaaS apps access control, and together with MAM, is the key element for distributing public and private apps in the mobile workplace. The usage of MDM or MAM containers also increases the level of data security and improves the user experience.

However MDM doesn't offer any potential threat detection, therefore, in order to have a compelling secured mobile workplace, Advance Threat Prevention (ATP) must be included working together with MDM. ATP protects devices from threats that come from the installed software (malware and unknown/Zero-day threats based on its behavioral analysis of processes). ATP must be automated with MDM in order to automatically trigger a policy when a threat is detected. It then needs to restore the device status once the threat has been removed from the device. It’s important that ATP includes features that monitor app stores using big data techniques (e.g. Tacyt) to proactively
avoid downloading suspicious apps onto the devices even prior to their installation.

When going mobile, mobile apps require different methods of authentication. For ease, integrating identity management through a single solution is the best approach. This implies that MDM containers, and mobile apps have an integrated authentication method (e.g. mobile connect).

The last component that plays an important role in securing a device is the VPN connection. The Digital Workplace must guarantee seamless VPN connectivity avoiding manual intervention of the end-user each time an app is forced to use the VPN. For this reason the MDM or MAM vendors’ smooth integration of per app VPN solutions and split-billing solutions is key.

**Productivity applications in the Digital Workplace**

Apart from security, already covered in this paper, there are other productivity apps to be taken into account when considering a Digital Workplace strategy.

A basic approach to Digital Workplace should include, at least, the following apps:

- Mail
- Cloud storage including secure content management for protecting critical data
- Secure web browsing
- Collaboration apps. Related to this, normally Lite versions of unified communications (UCC) apps
like Broadsoft, presence, instant messaging, or basic conferencing

■ VoIP dialer including, additionally local break-out

■ Internal company apps. This also includes, apart from native, or hybrid home-made apps, virtualized clients that permit remote launching of virtualized apps

■ Container with all the security features mentioned previously, normally provided by an EMM vendor (MDM or MAM)

As organizations go deeper into their digital transformation, full UCC systems such as Broadsoft or Cisco HCS environments can be migrated to the digital desktop. More and more customers are adopting strategies to remove fixed phones and merge those capabilities onto mobile devices. It’s relevant to consider, not only a standalone migration from hosted to cloud UCC, but also which role it would play in a Digital Workplace strategy in the mid-term.

Each area of the organization has to define their apps roadmap to be integrated in the Digital Workplace solution. This means:

■ Sales and fieldforce apps

■ Top management analytics and dashboards

■ HHRR apps (holidays or digital expenses management (Captio), workflow authorization)

■ Business process apps that contribute to digitizing the organization

■ 3rd party out-of-the-box apps to mobilize traditional desktop web access (Salesforce, Office 365, Trello, Noisy, Evernote)

---

**Figure 9: How can apps transform your business?**

How can apps transform your business?

<table>
<thead>
<tr>
<th>Increased</th>
<th>Decreased</th>
</tr>
</thead>
<tbody>
<tr>
<td>+63% Worker productivity</td>
<td>-63% Paperwork</td>
</tr>
<tr>
<td>+19% Service revenues</td>
<td>+13% Sales revenues</td>
</tr>
<tr>
<td>+50% Customer satisfaction</td>
<td>-31% Travel time</td>
</tr>
</tbody>
</table>

*Source: Technology Service Industry Association*
Authorize users must have the ability to properly assign apps per worker profile in order to optimize licensing costs.

**How Telefonica can help enterprises with their Digital Workplace**

The digital revolution presents both opportunities and challenges for all businesses, but avoiding the digital transformation can mean losing competitiveness, productivity, and over time, business decline. In this new Digital Workplace, mobility is fundamental for the new digital enterprise.

Historically, the main issue for the mobile workforce has been down to employees not having access to all of the information resources they require for their role. The objective of the Digital Workplace is to bridge this historical gap between wired and wireless network: anytime, anywhere complete access to the business through detachables and smartphone devices. By offering secure access to the business environment through mobile apps, employees can feel more empowered in their work with the ability to work how, when and where they choose.

The Digital Workplace provided by Telefonica Business Solutions goes beyond just the connectivity and includes the whole Digital Workplace lifecycle. Our best-in-class products developed by our innovation areas are created to offer enterprises end-to-end, secure mobility management, implementation and support, built around the requirements of our customers. Our brand new 4th Platform will also complete our offering and bring a differential value to our customers. The Digital Workplace is not only a set of outstanding functionalities and service performance but also a new business model based on OPEX, making it easier and more predictable to manage.

**Telefonica plays a key role as one of the global players in Enterprise Managed Mobility, one of the foundations of the Digital Workplace, recognized by Gartner as a Visionary in the Magic Quadrant for Managed Mobility Services, Worldwide in 2016, and for the third consecutive year.**

Source: Telefonica

---

1Gartner, Magic Quadrant for Managed Mobility Services, Worldwide, Katja Ruud, et al, October 2016
EMM tools are more powerful than many IT leaders focused on mobile strategy realize. Commonly deployed in narrow use cases to manage device configurations, their ability to rationalize and even reduce costs is unwittingly overlooked. EMM can offer positive returns beyond keeping devices in check.

Key Challenges

- Delivering configurations to mobile devices at scale and providing inventory information to speed problem resolution, EMM delivers cost benefits through lower operational overhead for teams supporting mobile workers but delivers little upside.

- Mobile and endpoint computing leaders deploy EMM tools to enforce security policies and enhance IT’s ability to support mobile platforms. While important, few organizations tap into EMM suites’ capability to generate cost savings or drive digital business activities.

- EMM tools often eschew the policies that can drive down carrier and software licensing costs in addition to the operational cost benefits they provide for IT.

Recommendations

- Expand EMM policies to drive cost reduction in three areas beyond basic MDM: Begin with tracking underutilized assets, and expand cost controls through telecom and software license controls.
Take advantage of EMM policies or integrate EMM data with an incumbent TEM tool to target asset and carrier costs like underutilized device assets, inactive lines of service and unexpected carrier cost overruns.

Track mobile app license compliance and utilization, target where to apply discounts, and understand LOB-led investment using native EMM controls or through integration among EMM and existing SLM tools.

Strategic Planning Assumption
By 2018, 80% of organizations that have deployed an EMM tool will fail to leverage its capabilities to drive down telecom, app licensing or asset utilization costs.

Introduction
Gartner finds companies that have invested in mobile device management (MDM) and enterprise mobility management (EMM) tools often limit deployments to basic tasks. Most organizations only use about 10% of EMM’s total functionality. These basic use cases, such as granting email and network access, enforcing a PIN code to lock an inactive device, or quarantining compromised devices to limit their access to corporate systems often provide little upside in reducing hard costs.

EMM is a necessary endpoint management tool, but one that can offer greater benefit if applied with a broader set of policies. Often overlooked by organizations using EMM and MDM as basic configuration management tools, expanding policies in three areas in addition to basic MDM can yield cost optimization (see Figure 1).

Figure 1. Use Four Types of EMM Policies to Optimize Mobility Costs

Source: Gartner (September 2016)

The ability to bring savings to the broader business will improve the profile and perceived value of a tool mobile and endpoint teams must deploy but that often lacks broad acceptance. Expanding use of commonly available EMM features can create a cost picture that drives the executive buy-in needed to deploy EMM widely and achieve the important goal of visibility into all mobile assets.

Analysis
Expand EMM Policies to Drive Cost Reduction in Three Areas
Gartner encounters countless organizations where EMM deployments have stalled. This leaves a portion of mobile users subject to little or no control over how corporate data is being used on devices, and how corporate-issued devices themselves are being used. The situation provides few assurances to management that all mobile devices are accounted for and that the corporate data on them is protected uniformly.
Maintaining continued investment in this critical, if often underappreciated, element of a mobile strategy depends on easing the IT-business friction inherent in an EMM deployment or expansion.

As EMM deployments move to include a greater set of policies, business value to the larger organization grows in correlation. An example of this is the business that brings on EMM as a single system to provide insight into multiple mobile device platforms. Initial benefits from this use case are largely operational and limited to endpoint support and operations teams. As the use cases grow to include deploying third-party and custom independent software vendor (ISV) apps, the value of the devices in the hands of users grows. As rules such as limiting the ability of a device to roam or using location-based policy to serve contextual information come online, the value proposition grows further.

EMM tools provide real-time visibility into mobile asset inventory, which helps IT organizations and end users remotely track devices under management. The data gathered from devices is invaluable. It helps IT recover missing devices from their last known location and redistribute those and underutilized devices to other users. Highly valuable in asset management, this capability is core to nearly all EMM tools’ dashboards, including base-tier offerings and some no-cost offerings. This can be seen, for example, in the Cisco Meraki dashboard. Meraki makes the MDM tool available as a SaaS console to enroll and manage devices for free for up to 100 enrolled devices.

Shared devices and shift work present other uses of EMM that can drive cost savings. In healthcare organizations that use tablets for recording and exchanging patient information at the point of care, for example, a single device can be handed off between roles (e.g., doctor, nurse and medical technician) and between shifts of practitioners. An EMM agent can allow for the device to be checked out at the start of a shift and checked in at the end, loading a given user’s personalized settings, apps and data at check-out and removing them at check-in. Using EMM to allow devices to reconfigure with zero user touch obviates the need to procure a dedicated device for every user. The same model can be replicated in other environments that employ shared devices or for static kiosk devices that can be reconfigured to showcase different information based on time or location, also using EMM policies.

Identifying misuse of devices is a side-effect of tracking using EMM dashboards, as noted above. However, it can also identify behaviors that indicate misuse of resources beyond the device itself, including corporate-provided data and voice plans. EMM tools can track SIM card tampering through compliance policies. Detecting a change of a SIM card tied to data plans renegotiated by the organization can identify misuse of the SIM and, therefore, data service in a noncorporate or other unsanctioned device. Policies can be designed to trigger notification or initiate a workflow based on removal or replacement of a SIM card.

Not all misuse is malicious; consider a real-world scenario where an employee inserts a roaming carrier SIM inside a managed device to perform functional testing and forgets to put back the home carrier SIM. This can lead to “bill shock” at the end of the month, as all calls made and data used during the period will be billed against the roaming SIM. EMM compliance policies to detect a SIM card change can prevent this cost overrun.
Use EMM Policies to Target Telecom Costs From Underutilized Devices, Inactive Lines of Service and Minimizing Unexpected Carrier Cost Overruns

Beginning the EMM makeover from cost to value driver starts by tapping into capabilities native to even the most basic MDM and EMM offerings from leading EMM vendors. In their most basic form, EMMs can generate asset utilization metrics through dashboards showing devices in use and devices per user. EMM suites can take an active role in controlling telecom costs through near-universal support for native iOS and Android controls that can place restrictions on data usage by apps or based on environment.¹

Examples of Cost Optimization Outcomes Based on Cellular Policies in EMM

Controlling roaming costs: The cellular state of a smartphone or tablet can be used as a policy trigger for many aspects of a mobile device’s functions. These include restricting automatic syncing of information on the device when roaming and restricting data usage altogether when roaming, as well as policy to avoid costly and unexpected carrier charges when users are roaming. EMM can further place controls on the user’s ability to enable cellular roaming.

Managing cellular data usage: Both iOS and Android allow configuring managed devices with cellular policies that govern mobile data usage. Consider applying cellular data restrictions for managed apps that are not mission-critical. Note that these restrictions don’t apply to personal apps. IT can disable mobile data usage on the home as well as roaming network. EMM tools also provide ways to track data usage and set thresholds on maximum SMS and voice calls.

Restricting network usage: EMM tools also provide the ability to guide content downloads to preferred networks, such as Wi-Fi over cellular, as a complement to some of the restrictions outlined above or as a stand-alone policy. Examples include content-centric apps, such as a mobile content management (MCM) tool, providing controls to prevent syncing on a cellular data connection. Some EMM tools also include video apps. IT should ensure that it enables the settings to download videos only on Wi-Fi to minimize unnecessary mobile data usage.

Track Mobile App License Compliance and Utilization, Target Where to Apply Discounts, and Understand LOB-Led Investment

Gartner defines a mobile application management (MAM) tool as an on-premises or SaaS tool specifically designed for the license management, distribution, securing and life cycle management of apps for mobile device platforms. As organizations deploy mobile apps to improve their business processes, there is an associated cost tied to many of the apps they look to deploy after addressing the use cases of email, contact, calendar and MCM. For instance, cloud office productivity tools, such as apps in suites like Microsoft Office 365, provide near-universally applicable productivity on mobile; however, use of these no-cost apps for business purposes requires a specific Office 365 subscription, making tracking of usage and application of proper account credentials imperative.

EMM’s role in managing software license spans inventory, license compliance and optimizing utilization. Three example policies can be applied as follows:

- Enforcement of app whitelists: Creating mobile app “blacklists” of apps not approved for use on a company-owned device creates overhead in the
form of maintaining lists in the face of rapid app marketplace growth, making this untenable as a manual task. Automating blacklist maintenance may require additional investment. Instead, focusing on the small and often-finite set of required apps for users through establishing an app “whitelist” that can be enforced through EMM can head off unwanted behaviors and access to specific, inappropriate content. This option should only be exercised where a limited set of apps is in use and no personally owned devices are in play.

- **Mobile app license management:** This can be divided into two parts – underutilization and overruns of app licenses. Apple’s Volume Purchase Program (VPP) and Google’s Google Play for Work, for example, allow for bulk purchasing, assignment and tracking of licenses for paid apps. Using EMM tools to maintain inventory of apps, centralize license management, and reassign licenses to new users or devices can reduce inactive licenses, cut down on expensive approval overhead for app purchases and reduce duplicate purchasing (see Note 1).

- **App license utilization management:** In addition to gaining better visibility into app license assignments and utilization, some organizations use the reporting function of their EMM to better understand the utilization of organization-provided or subsidized devices. Using default dashboards and commonly available reporting components of an EMM console, organizations can identify devices and lines of service that are dormant or underutilized and represent a potential area for cost savings.

**Evidence**

1. Apple implemented MDM controls that are available for management vendors to make use of in versions of its mobile OS going back to the release of iOS 7 in 2013. An expanded set of app-level controls was released for Google’s Android as Android for Work (AfW) in 2015 as part of enhancements to version 5.0 of Google’s mobile OS. iOS MDM controls currently enjoy broader support across EMM and MDM solutions, though Gartner has witnessed the number of tools supporting AfW grow rapidly and expects this to continue. Hampering widespread support in enterprises for AfW is the convoluted, multiparty nature by which many Android devices receive updates with wireless carriers and device OEMs empowered to approve or reject a given set of features of OS versions for customers’ devices.

2. Gartner recommends careful evaluation of the number and type of controls enacted on personally owned devices in contrast to those owned by a company or organization (see “Implement BYOD, CYOD and COPE to Serve All Employees”).

**Note 1**

**Apple iOS Platform**

Apple iOS platform supports app licensing at both a device and a user level. Direct assignment of apps to devices is cost-effective when devices are shared among multiple users, whereas user-level allocation of apps is handy when you want to reassign apps among users without buying additional licenses. To read more about Apple’s Volume Purchase Program and app management enhancements to iOS 9, see “What iOS 9 Means for Enterprises Using EMM.”

**Source:** Gartner Research, G00314781, Chris Silva, Manjunath Bhat, 12 September 2016
About Telefonica Business Solutions

Telefonica Business Solutions, a leading provider of a wide range of integrated communication solutions for the B2B market, manages globally the Enterprise (Large Enterprise and SME), MNC (Multinational Corporations), Wholesale (fixed and mobile carriers, ISPs and content providers) and Roaming businesses within the Telefonica Group. Business Solutions develops an integrated, innovative and competitive portfolio for the B2B segment including digital solutions (IoT, Cloud, Security) and telecommunication services (voice, data, mobile, satellite, unified and global solutions). Telefonica Business Solutions is a multicultural organization, working in over 40 countries and with service reach in over 170 countries.

https://twitter.com/TelefonicaB2B

Contact us

For more information contact us.