IBM Security
Thought Leadership Article

June 2016

Unified Mobility Management

Enterprise mobility tools have evolved to the point where a single unified cloud platform can manage everything from phones to tablets, PCs and even remote sensor devices.

IBM

Modern workforces are mobile. In fact, that's the new normal in most of Australia and New Zealand, where enterprise mobility maturity is highest in the Asia-Pacific region, according to IDC Research.[1]

Eventually every business and government department around the world will be entirely mobile all of the time. Some organisations in Australia and New Zealand are already close to that point. Their employees use phones, tablets and laptops to work on the move, meaning every day they deal with a variety of wireless networks and mobile computing services.

Working this way brings huge benefits. It leads to new levels of customer responsiveness and makes for agile, fast-moving organisations that are well placed to seize opportunities as they arise.

Yet, since the first iPhones appeared in the workplace in 2007, businesses have struggled to integrate mobile technology with their work processes and objectives. They have also found it hard to give mobile employees the support they need.

Help first came in the form of mobile management tools. Early tools were point products developed to address specific concerns such as mobile security, identity management and expense management.

These solutions were often high quality and provided the needed functionality. The downside was, while managing one or two point solutions was straightforward enough, they quickly multiplied. This made management more difficult, with complexity growing exponentially as more functionality was added. Not surprisingly, IDC's 2015 Enterprise Mobility Survey showed that more than half of all respondents said they were not happy with the tools on offer.[2]

In response to user demand, enterprise mobility management (EMM) suites were introduced to reduce the complexity. In effect, EMM pulls together the functionality of point solutions into integrated packages. These platforms not only handle functions such as device configuration and security policy management, but also deal with mobile apps, content strategy management and access to corporate information resources.

EMM suites have a single user interface, and organisations can manage all the functions from a central point, often a dashboard. Enterprise mobility is still at an early stage and therefore fast moving. No sooner had EMM established itself as the standard, the need to expand management functionality and further reduce complexity emerged.

One challenge for IT professionals charged with overseeing enterprise mobility is controlling total cost of ownership (TCO) for each device under management. In a period of just five years, from 2015–2020, mobile data traffic was expected to grow eight-fold.[3] This may not sound high, but with an explosion in the number of endpoints being managed, the overall cost can quickly spin out of control.

In response to spiralling TCO, unified mobility management (UMM) platforms like IBM's MaaS360 have emerged. These platforms not only improve integration, but also add support for a wider range of devices, including PCs. Overall, UMM promises users the ability to perform more tasks using fewer resources.

UMM suites typically support Windows PCs and Macs, including those running older operating systems. They can also be extended to embrace remote Internet of Things (IoT) sensors and devices.

Because UMM brings a range of devices under one umbrella, there is no need to maintain parallel support infrastructures for mobile devices and PCs. This can dramatically reduce per-device TCO, enabling organisations to use the savings on apps to automate the mobile management process. This not only makes organisations more agile and responsive, but also opens the door to further productivity gains.

Cloud is central to UMM. It delivers all the necessary functionality, including patching, maintenance and training. To an IT professional supporting mobile users, UMM cloud platforms look like familiar software-as-a-service (SaaS) applications, where mobility is controlled by a single user interface. Such automated cloud services free IT professionals to focus on more strategic matters, such as policy management and leveraging other productivity benefits.

Analysts such as Gartner recognise IBM MaaS360 as a leader in the UMM space. The cloud-based platform supports iOS, Mac OS X, Android, Windows Phone, Windows 7, Windows 8 and Windows 10. Key to its success is the ability to manage everything mobile on a single platform, bringing all endpoints under one umbrella. MaaS360 also offers features such as expense management and built-in mobile threat protection.

Mobile can be relatively secure, but there are still serious threats. For example, Android phones are especially prone to the risk of unauthorized apps with malware payloads, and there are many rogue Wi-Fi hotspots in crowded areas like airports and railway stations. With the average cost of a third-party cybersecurity attack in Australia now averaging approximately A$400,000, the need to secure endpoints has never been greater.[4]

There are four main UMM use cases. The first two are straightforward: company-owned devices and bring your own device (BYOD). Use of company-owned devices remains the most common model. The third use case is shared devices, whereby a worker signs out at the end of a shift and passes a device over to a colleague. This is common in industries such as healthcare, where nurses, for example, might share devices.

The fourth use case is when contracted workers are given tools to perform certain tasks and might have devices for only a limited time. This is increasingly common with government and private companies hiring contractors to meet short-term staffing needs.

EMM would be complex enough even if each employee were restricted to a single device. That's increasingly rare, however: Even in conservative organisations, the average number of devices per employee is 1.5. And it's not uncommon for some workers to carry more than one phone. Add PCs to phones and tablets and the number of devices per employee is closer to 2.75. Again, it's not unusual for that number to be higher.

Recommendations

For more effective enterprise mobility management, organisations should partner with an experienced UMM vendor. Look for one able to work neutrally across the major mobile and desktop operating systems. Success depends on being able to provide support for all the most popular user devices in heterogeneous environments.

One benefit of cloud-based UMM is that, like any other SaaS environment, it is simple and quick to implement. SaaS is also flexible, so the best vendor partners will be able to offer a test drive before you commit to their platform.

Implementing UMM will give you the opportunity to greatly simplify your enterprise mobility operation—and it's wise to make that move today given enterprise mobility will become only more complex later.

UMM means you'll be able to reduce TCO before it spins out of control. You'll also be able to offload low-value tasks to SaaS, better control mobile data usage and guard against security risks.

Because UMM is cost effective, your organisation will realise savings that can be invested in vertical mobile apps that further automate management processes, enabling greater agility and higher productivity.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
March 2016

Please Recycle

References

1 "Mobility Solutions Key to Reeling in $3 Billion of Spending in Australian Healthcare, Finds IDC," IDC Research, 02 Sep 2015

2 "Asia/Pacific Enterprise Mobility 2015: Moving Beyond BYOD" [Infographic], IDC Asia/Pacific, Nov 2015

3 "Cisco Visual Networking Index: Forecast and Methodology, 2015–2020," Cisco, Updated 01 June, 2016

4 "Webroot 2015 SMB Threat Report," Webroot, Dec 2015

TechTarget Custom Media

WGW03116-USEN-01