computing research

RESEARCH PAPER

Mobility must-haves: UEM, cyber security, and productivity for the distributed workforce

November 2020

Sponsored by

O2 SAMSUNG

CONTENTS

Introduction

IT leaders have been gradually turning to cloud-based mobile device management tools for years, swayed by the convenience of remote updates, policy control and security. Their IT teams were typically overworked, with an increasingly diverse and large technology estate to manage, so anything that could ease this burden was welcomed.

The widespread shift to remote working during 2020 has only accelerated the growth of these priorities and challenges. Administrators need to be able to distribute, secure, manage and support mobile devices wherever they may be, from their initial setup at home, to their eventual return to the traditional workplace. They also need to ensure that security and access policies are up to scratch, in the face of the cyber threats imposed by distributed workforces – whether remote, travelling or in an office.

Computing surveyed 150 decision makers who are involved in mobile endpoint device decision making or implementation at organisations that provide mobile devices to their employees. These individuals represent organisations from a wide variety of industries including banking and finance, logistics, manufacturing, retail, and the government sector. The objectives of the research were to explore the key mobile priorities amongst organisations today, the challenges they are facing, and what they look for in a vendor partner. What does a Unified Endpoint Management (UEM) platform need to be capable of today? And is a broader end-to-end service now a must have for mobile?

Key findings

- The most important selection criteria for devices were security/compliance, total cost of ownership and manageability.
- 86 per cent of contributors to our survey agreed, either somewhat or strongly, that the increase in remote working had made robust enterprise mobile cyber security even more crucial.
- Universal Endpoint Management (UEM) deployment has increased sharply throughout 2020. 53 per cent of contributors have at least begun to roll out UEM, and 37 per cent have completed this. A further 31 per cent are either trialling solutions or in the planning stages.
- Organisations expect a great deal from their UEM. The average score out of 10 for an array of features was 7.5. The most highly valued features were remote lock and data wipe, data access permissions and encryption, and compliance checks.
- When selecting a partner and/or device vendor the most important criteria are costs and transparency of cost, followed by ease of contact/working relationship and support levels.
- More than half – 56 per cent – of contributors required an end-to-end service encompassing device deployment, security and management, from their mobile vendor partners.

Return to normal – a remote possibility

Pre-pandemic, organisations were already experiencing challenges trying to manage and secure a rapidly proliferating number of endpoints. A generally increased trend for remote working, the availability of applications on cloud platforms, the sharp rise in IoT devices, and the perennial cycle of update testing and deployment were all combining to make endpoint management more of an issue.

The pandemic-induced shift to widespread remote working in March 2020 happened extremely quickly. This created extraordinary challenges for organisations having to secure the activity of employees who were not used to working solely from home and posed a greater risk to the cyber security and compliance of organisations as a result.

A brief respite over the summer months allowed a little more normality in terms of returning to offices, and a little breathing space for organisations. However, having invested considerable resources on the rolling out of widespread remote working, and noted the unsuitability of many traditional office layouts for social distancing, many organisations followed the lead of the technology giants and ignored the UK government advice to return to their places of work. This showed a degree of foresight because in the UK, the advice to return to the office was rescinded at the beginning of Autumn, and working from home as the norm for all those who are able to do so seems set to continue well into 2021.

Whether the prevalence of remote working will recede alongside the pandemic is a point of debate, but as long-term lease agreements on workplaces expire over the next few years, it is likely that a degree of office space downsizing will occur – at the least. Therefore, the role that remote working plays in the overall way that we live and work is unlikely to diminish to any significant degree. Consequently, all aspects of remote work are under the microscope – the devices themselves, connectivity, how you secure and manage those devices, your data and your applications.

Device considerations

All the organisations taking part in our research provided mobile phones to their employees. 44 per cent provided phones for "some," employees, 33 per cent for most of them, and 23 per cent to all.

Fig. 1 : On a scale of 1 (not at all important) to 10 (extremely important), how important are the following when selecting mobile devices for your organisation?

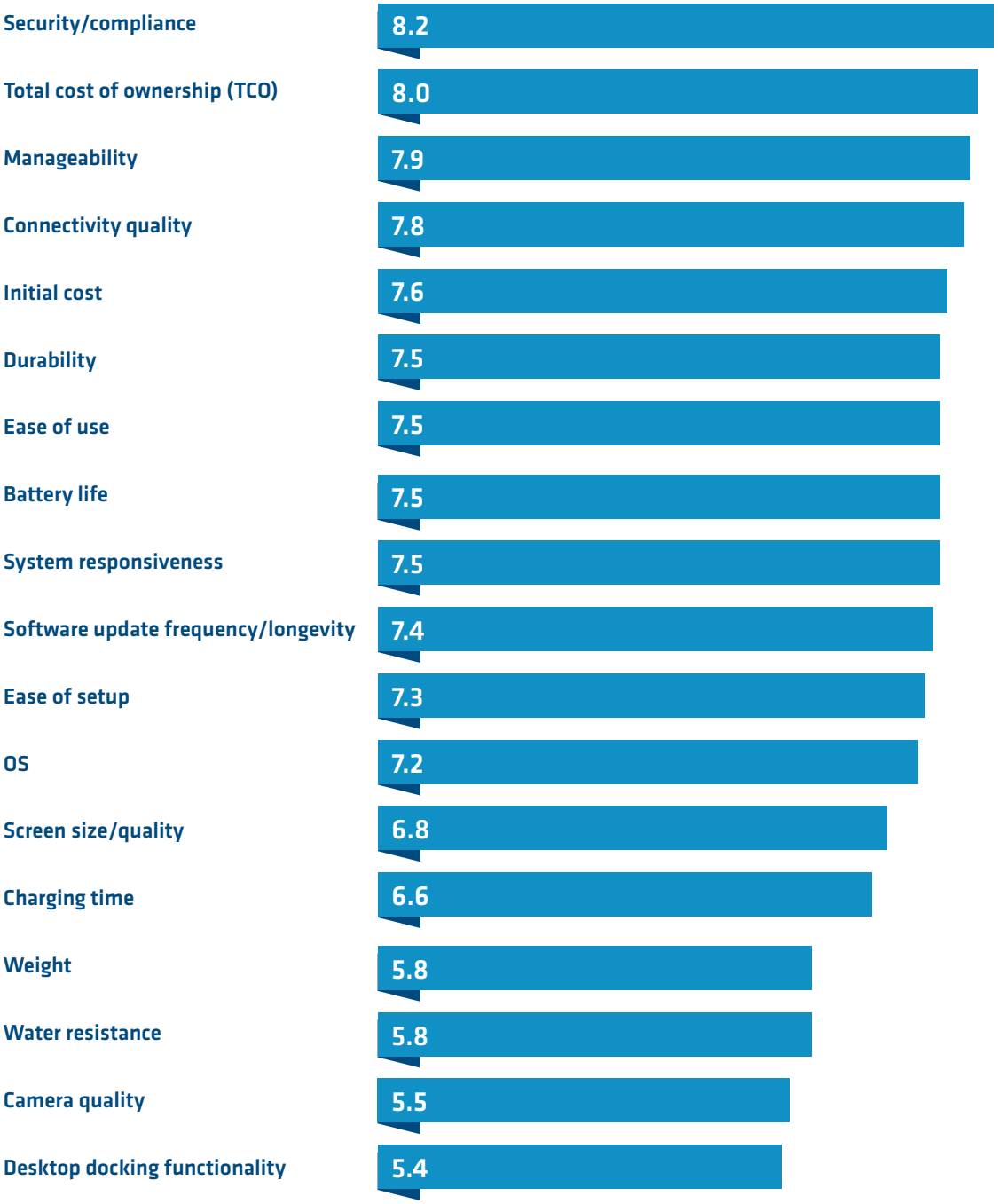


Figure 1 sets out the characteristics that businesses look for when they choose mobile devices to issue to their employees. Of little surprise to anyone will be the importance of security and compliance which topped the list by a reasonable margin. 86 per cent of contributors to our survey agreed, either somewhat or strongly, that, "the rise of remote working has made robust enterprise mobile cyber security even more crucial."

Cyber criminals were not slow to exploit the sudden explosion in remote working, and Computing's own research has shown an increase in phishing activity exploiting current affairs to lure people into downloading ransomware or other malware. Phishing lures are also exploiting the increasing traction of conspiracy theories about COVID-19, and a recent campaign in the US has used voter registration for the presidential election as bait. Most employees probably know they should be wary of these kinds of emails, but it's difficult to be certain that your employees won't be tempted just for a moment. Given that so many individuals are working at home, there is also the possibility of devices being borrowed by other family members. Meanwhile, the home networks that work devices are being connected to are far less secure than those in the office.

Another aspect of the security and compliance imperative is the use of consumer-focused public web file sharing services – and the placing of corporate data into these services. This is not a new problem. Employees tend to default to the user-friendly consumer applications that they are already familiar with, rather than using the officially sanctioned collaboration and file sharing platforms. Some businesses have dealt with the issue of third-party applications via UEM or application control software, whitelisting, and corporate app stores. Or simply removing administration rights for users, which works but at the expense of a lot of extra help desk calls. Employees often also work around the problem by using their own personal devices instead. This is also a far from ideal scenario. Many organisations are still relying on policy-based controls and the self-restraint of users and their knowledge of the implications of running unauthorized software.

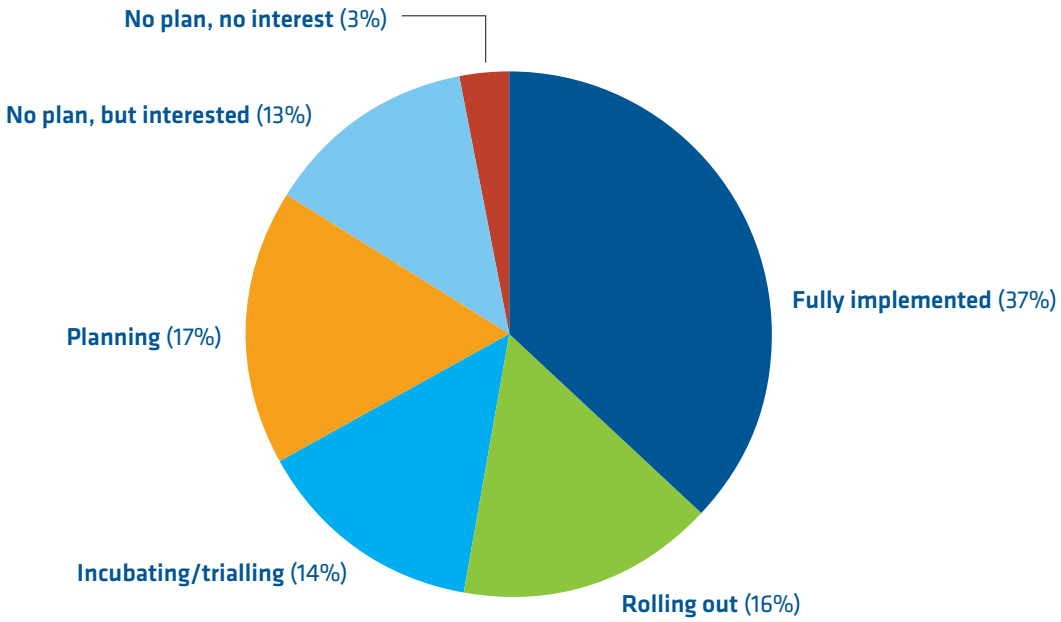
Total cost of ownership (TCO) was also a prime consideration, and understandably so. The purchase of mobile devices is just the beginning of a lifecycle of cost – management, application control and security, and OS updates. Tied into the issue of TCO was the third most frequently cited factor – manageability.

There is an array of mobile devices out there. Given the critical importance of cyber security, data on devices should be encrypted by default, both when devices are powered off and also when in a powered on but locked setting – which tends to be the state devices are in when they are lost. Devices should also have security and compliance policies applied accordingly. They must be able to pull off the trick of being zero trust, whilst empowering users to be productive. Zero trust, continuous authentication should allow users to do their jobs without generating multiple helpdesk calls, or users feeling as if they are being treated like liabilities who need to be monitored.

The importance of UEM

There is, of course, far more to the security of mobile devices than the device itself. Organisations have been increasingly turning to Unified Endpoint Management (UEM) to resolve some of the challenges that the explosion in the number of endpoints has created for them. Figure 2 shows the extent of its popularity. When Computing asked similar questions in Spring 2020, the proportions having already implemented UEM were noticeably lower, suggesting that pandemic conditions have boosted UEM deployments considerably. We are now at a point where 53 per cent of contributors have at least begun to roll out UEM, with a further 31 per cent either trialling solutions or planning them.

Fig. 2 : Does your organisation use a Unified Endpoint Management (UEM) platform to manage its mobile devices?



UEM goes a considerable way to helping organisations to manage the issues that they identified when assessing devices themselves – namely security and compliance, TCO and management. IT service management and cyber security professionals can use a single management console and can interrogate a single source of data in the event of a suspected issue. Management and security can all be managed from one place and for end users it's business as usual. The reduced management burden then reduces overall TCO.

The data in figure 2 suggests strongly that UEM is more than a 'nice to have' technology. 75 per cent of our contributors agreed either somewhat or strongly that, "the rise of remote working has made a capable UEM solution essential to the effective management of enterprise mobile devices."

What are businesses looking for in their UEM solutions? Figure 3 tells us that the most desired functionality is remote lock and data wipe functionality – which is crucial if a device is lost, stolen, or compromised by malware.

Fig. 3 : On a scale of 1 (not at all important) to 10 (extremely important), how important are the following capabilities in a UEM solution for your mobile devices?

The high priority of encryption is an interesting finding because capability does vary. Devices with single layers of encryption are inherently less secure than devices where data is encrypted twice, using separate systems. A dual encrypted device is better protected against administerial oversight, operator errors or straightforward malicious attacks.

Compliance checking is also an interesting finding. There is value in a mobile management solution which blocks or at least restricts access to enterprise resources if the device falls out of compliance – criteria for this being determined by the administrator. However, the kind of issues likely to lead to a device falling out of compliance – OS version, patches and updates, and rogue applications – are less likely to occur in the first place if a UEM solution is in play because these things can be pushed out and policy enforced centrally.

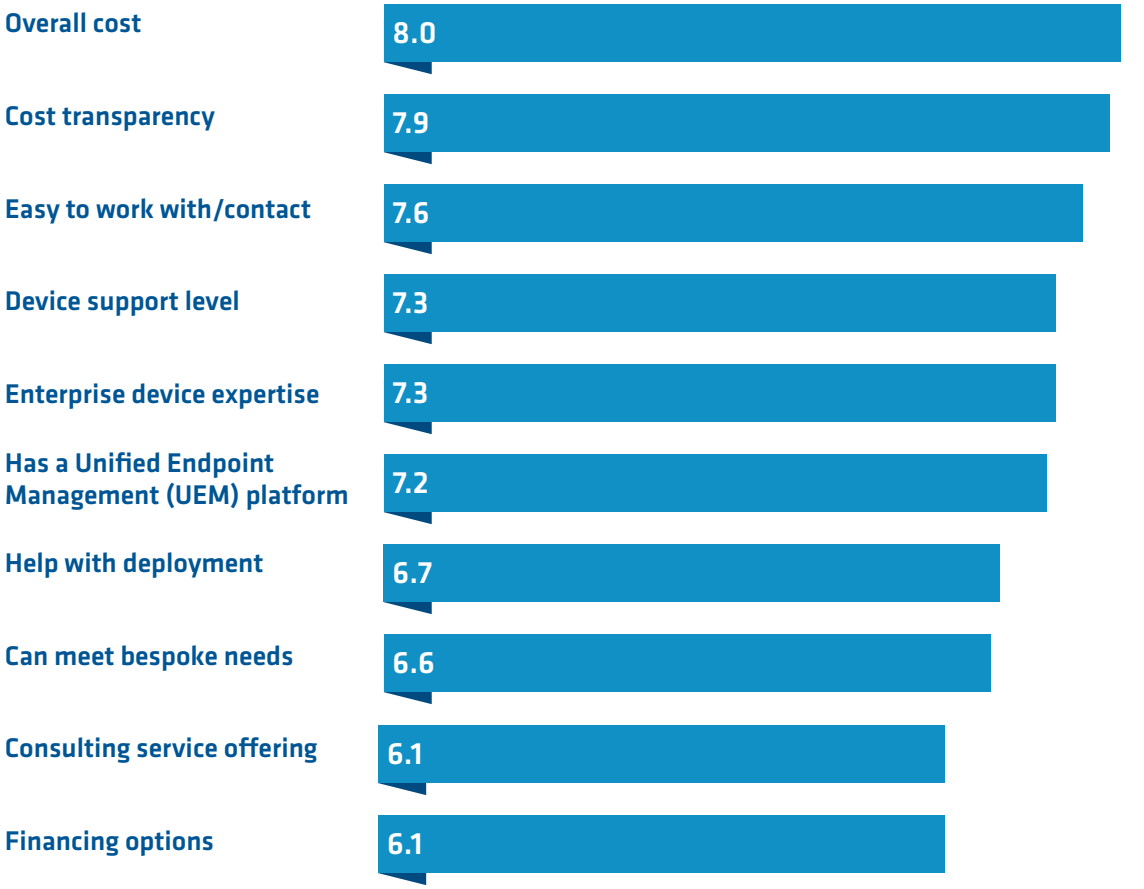
When looking at the list of features in figure 3, it is worth noting the overall high average score of 7.5. Very few features polled less than a 7 out of 10. Enterprises demand feature rich UEM, including capability such as remote deployment, whereby client installation and enrolment can be automated – particularly important during a time of near-universal remote working and the need for social distancing.

Selection of mobile vendors – and the benefits of consolidation

There are many factors to consider when choosing a vendor of mobile solutions. Figure 4 sets out the priorities of our contributors. Continuing the theme seen for the devices themselves, the first two priorities relate to cost – both overall and transparency thereof. The next highest scoring factors of easy to work with/contact and device support levels are also related to matters of cost, specifically TCO. The importance of support quality in the enterprise market should not be underestimated. 60 per cent agreed to at least some extent that "the quality of support and consulting provided by a mobile device partner are as important as the device itself." Only 13 per cent of respondents disagreed to some extent with this statement.

Organisations are much more likely to tick all these boxes, and receive keener costs, by consolidating their mobility requirements. Choosing a mobile vendor who can also provide support, security, provisioning and management tools from a single interface is likely to have a positive effect on TCO. This effect is magnified if devices and UEM solutions are procured via connectivity vendors, so billing and consumption data for different types of WAN, as well as mobile, can all be managed centrally. It is also intuitive to place the security of mobile devices and data into the remit of either the device or connectivity vendor, depending on the degree of integration with UEM available. This removes the cost and time involved in managing multiple vendors and platforms to secure differing aspects of different devices.

Fig. 4 : On a scale of 1 (not at all important) to 10 (extremely important), how important are the following when selecting a device vendor/partner?



An end-to-end enterprise mobility provider can provide a superior quality of service when compared to the alternative of a patchwork of mobile deployment, management and security tools. This quality of service is as important as the devices themselves.

Conclusion

The number and diversity of endpoints being deployed, secured, and managed by enterprises in the UK has been growing strongly for several years. This growth trajectory became steeper as 2020 progressed, as businesses roll out remote working to more and more employees. The connectivity, and the security and management of these endpoints are all under consideration as our ever more distributed human workforce moves into 2021.

When choosing devices, our contributors' top priorities were security and compliance. This was likely to have been the case before 2020, but the pandemic has brought about some extra security challenges due to the sharp increase in remote and home working. Contributors were also concerned about the total cost of phones throughout their lifecycle and the manageability of devices.

UEM is one way that our contributors have been managing the challenges that the explosion in endpoints has created. More than half had already begun to roll out UEM, and 37 per cent had already completed it. A further 31 per cent were in the trial or planning stages.

Three quarters of respondents considered UEM to be essential to the effective management of enterprise mobile devices. The faith that cyber security professionals have in remote workers is clearly patchy, because the most desired attribute in a UEM solution was remote lock and data wipe functionality. Strong levels of encryption and compliance checking are also widely valued attributes.

The biggest priorities for organisations when evaluating mobile devices is cost – including initial cost, longer-term TCO and transparency of costs. The ease of contact with vendors and support levels are also key.

In summary, enterprises want the highest security standards for their networks of mobile devices, as well as excellent value for money. Organisations can increase the chances of this outcome by choosing mobile devices, platforms and UEM suites via a single vendor. You can't secure what you can't see, so the consolidation of support, support, security, provisioning, and management tools into a single interface enhances both security and visibility of mobile infrastructure – the two are inextricably linked. It also enhances TCO, thanks to the time and cost savings available from consolidating multiple vendors and platforms.

If devices and UEM solutions are procured via connectivity vendors, billings data for different types of WAN as well as mobile can all be viewed from a single interface. More than half of our respondents want this degree of consolidation. 56 per cent agreed to some extent that they "require an end-to-end service from my mobile vendor partners." Only 15 per cent of respondents disagreed with this statement.

Viewing enterprise mobility as an end-to-end process rather than the more traditional patchwork of deployment, management and security tools can boost quality of service for employer, employee, and their own customers. Consolidation is an excellent way of ensuring that the security and productivity of a distributed workforce do not have to be mutually exclusive.

About the sponsors, O2 and Samsung

O2 is a leading mobile network operator and the principal commercial brand of Telefónica UK Limited, part of the global telecommunications group Telefónica S.A.

An award-winning network and service provider, for three consecutive years, O2 has been named uSwitch Best Network Coverage provider via public vote (2018, 2019, 2020) and has over 34 million connections across its network. Combined with Samsung's rugged and secure devices, O2 have the proven tools, technology and support to give organisations the agility and governance needed to thrive.

Operating 2G, 3G, 4G and 5G services across the UK, as well as providing a nationwide O2 Wifi service, the company is the network of choice for mobile virtual network operators such as giffgaff, Sky Mobile and Lycamobile as well as managing a 50:50 joint venture with Tesco for Tesco Mobile. Together with Samsung's Knox solutions for Enterprise, business needs for security, deployment and device management are met with maximum control and productivity.

O2 has around 6,700 employees and over 450 retail stores and sponsors England Rugby, The O2 and 20 O2 Academy music venues across the UK. Through a comprehensive sustainability strategy O2 is also creating work experience opportunities for 16-24 year olds via its GoThinkBig platform, enabling customers to reduce their impact on the environment by recycling their old devices through O2 Recycle and, in partnership with the NSPCC, helping parents to keep their children safe online.

Mobility must-haves: UEM, cyber security, and productivity for the distributed workforce

Thanks to Samsung's reliable range of rugged devices, O2 can add an extra layer of protection to your operation. Samsung's Enterprise Edition integrates effortlessly with the Knox Security suite, streamlining configuration and deployment, installing security into the very core of employees' individual devices and contributing to a robust management and security process.

O2 is the only mobile operator in the 2019 Social Mobility Employer Index and was named as one of the best places to work in the 2019 Glassdoor Employee's Choice Award.

**Telefónica UK Limited is registered in England and Wales. Registration number: 1743099 and is headquartered in Spain and operating in Europe, and North, Central and South America. O2 is registered office is at: 260 Bath Road, Slough, Berkshire, SL1 4DX, United Kingdom.*