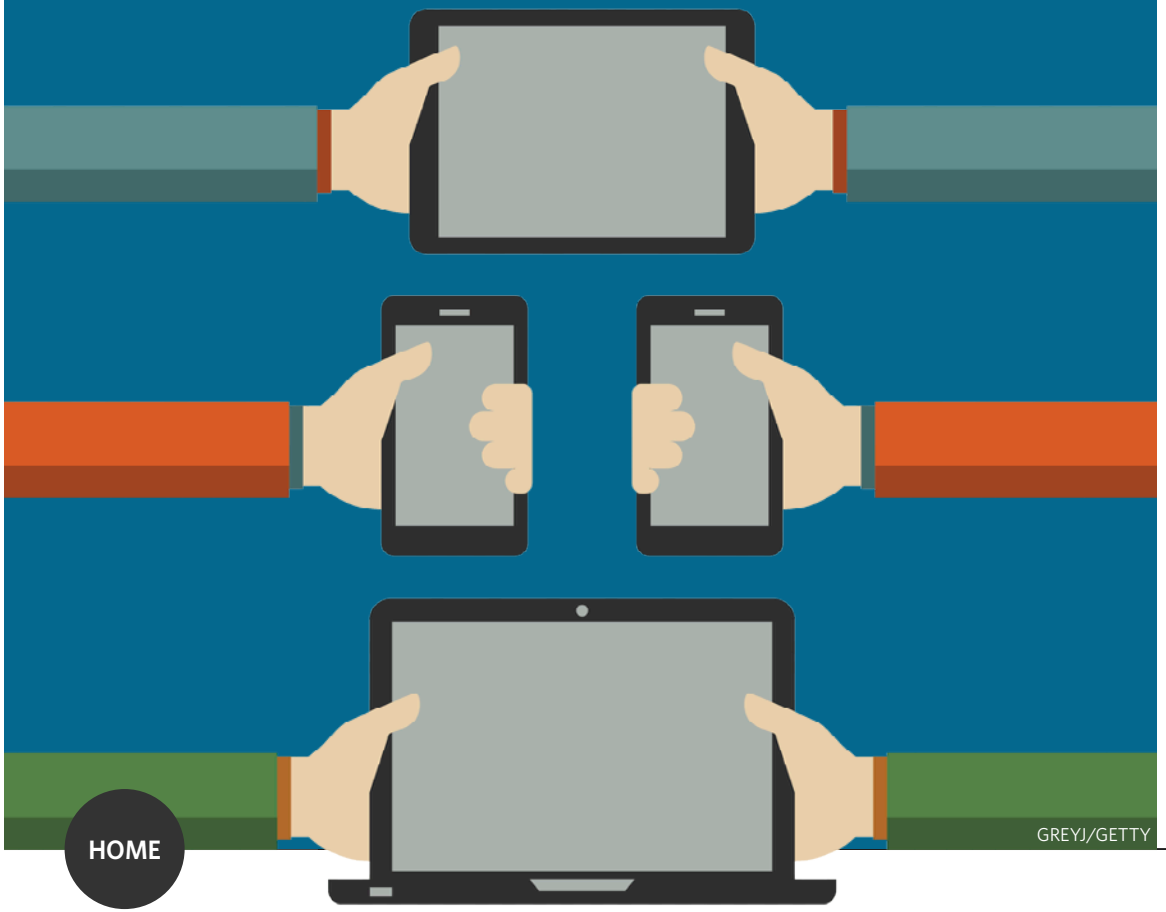
THE VALUE OF UNIFIED ENDPOINT MANAGEMENT

Given the diversity of devices people can use for work, IT needs to look at how it can unify device security, writes Bob Tarzey



GREYJ/GETTY

HOME

Ever since the advent of client-server computing in the 1980s, there has been a need for IT teams to manage user endpoints. In the early days, these were nearly all desktop personal computers in fixed locations running Microsoft Windows. The task started to become more complicated with advent of notebook PCs and easy remote internet access in 1990s and then with then the arrival of smart mobile devices in the last few decades, including wearable devices.

There has also been an explosion of non-user devices with the roll-out of internet of things (IoT) applications; sensors, probes, cameras, and so on. And, of course, traditional devices such as file servers and printers have not disappeared. The volume issues associated with endpoint management are exacerbated by the ability to virtualise many devices where their physical location does not matter.

For users, diversity means flexibility: the same applications and data could be accessed from any device anywhere. For IT teams, life has become more complicated: more devices, diverse operating software, increased security threats and, to cap it all, multiple management tools. What they needed was a single console to manage all endpoints. So how far has the IT industry come in delivering this through what has become known as unified endpoint management (UEM)?

BEFORE UEM: TOO MANY ACRONYMS

The terms used by the industry over the years have been confusing. The first tools were mainly developed to manage PCs; retrospectively, some people have called these client management

tools (CMT). These churned out golden images of corporate-defined Windows desktops, ensured they were patched, vulnerability-free and maintained inventories of hardware and software. In parallel, rising concerns about IT security were leading a new range of endpoint security tools.

The need to manage mobile phones led to a new and distinct set of tools for mobile device management (MDM). In the early days, these were as much about telecoms expense management addressing contracts, airtime services, subscriber identity modules (SIMs) and payments, as the devices themselves. As mobile phones evolved into smartphones, new challenges arose: bring-your-own-device (BYOD), user-owned equipment being used to access corporate resources, and the abundance of new software that users could download directly from app stores.

A confusing set of additional acronyms appeared: mobile application management (MAM), mobile expense management (MEM), mobile threat management (MTM), mobile identity management (MIM), mobile content management (MCM). For a while, the term enterprise mobility management (EMM) was settled on to cover all of these. Now, CMT and MDM/EMM have come together as UEM, so let's hope it's the final acronym.

UEM aims to reduce the cost and complexity of endpoint management by providing a single console, automating many management tasks and, with such holistic oversight, improving security. The features of any given supplier's UEM tools will vary, but some basics must be there.

> *While cloud endpoint security products, such as antivirus software, provide many benefits, the cloud connection also introduces risks.*

These include device discovery and inventory, asset management, remote provisioning and configuration, and lifecycle management with the necessary approval workflows and user self-service. Software licences and their distribution need managing. On user devices, this includes productivity apps such as email, calendars, contact management, document editors and social media, which must be used appropriately and securely. All this must be achievable across large volumes of devices, in some cases running in to the tens of thousands.

The range of devices will vary from one organisation to the next, including servers, desktops, notebooks, smartphones, tablets and printers, as well as the more esoteric devices that often coming under the IoT label. The number of operating systems has increased markedly beyond Windows. Android and Apple's iOS dominate on smartphones; Linux, Chrome OS and MacOS are used on larger form devices, and new operating systems have emerged to support IoT roll-outs such as QNX, Tizen, Android Things and Windows 10 IoT.

THE FEATURES OF ANY GIVEN SUPPLIER'S UEM TOOLS WILL VARY, BUT SOME BASICS MUST BE THERE

Support for BYOD must safeguard corporate data, ensuring business and personal apps are segregated on the same device. Apps can also

be whitelisted (allowed), blacklisted (banned) or greylisted (suspect) and app wrapping can modify the way apps work. This must extend to the use of cloud services accessed by users, such as file storage and sharing. This can be done using containerisation to separate corporate and personal use, controlling the flow of business data to and from devices, providing data analytics for insights into user behaviour. Encryption of stored data must be enforced as and where necessary.

Security must protect corporate systems against unknown endpoints. Some would go further and suggest all endpoints are treated as hostile; a known endpoint reconnecting to the home network may have been compromised while connected elsewhere.

Other security features should include basic anti-malware, secure web browsing and URL filtering, remote locking and/or wiping of compromised devices, GPS tracking and location-based policy controls, detecting when devices have been jailbroken, and identity and access controls such as user authentication.

Market convergence

Most suppliers that claim to be in the UEM space come from one of the pre-existing disciplines CMT, endpoint security or MDM/EMM. None of the main offerings has been designed from scratch as a UEM. In some cases, heritage strengths remain clear; in others, acquisitions or new developments mean equal strengths in multiple areas.

Most suppliers deliver UEM as on-premise software, cloud-based or a hybrid mix of the two. The way this is done will vary and different suppliers will be stronger in one delivery mechanism

Twenty features to look for in UEM

GENERAL MANAGEMENT
- A single console
- Asset management
- Software licence management
- Software patch management
- Roll-out of golden images
- Remote provisioning
- Approval workflows
- User self-service
- High-volume device management
- Device discovery

SECURITY
- Containerisation
- Vulnerability management
- Encryption and data protection
- Anti-malware
- Secure web browsing
- Remote locking/wiping

MOBILE SPECIFIC
- BYOD support
- Telecom expense management
- Airtime contract management
- App management

or another depending on their background. The direction of travel is from on-premise to cloud, although certain sectors, such as financial services, still prefer to keep things in-house.

Those with a CMT background include Microsoft, which now offers heterogeneous UEM via its System Center Configuration Manager (ConfigMgr) and Microsoft Enterprise Mobility and Security (EMS), which includes its Intune cloud service. Citrix has its XenMobile console for UEM and in 2017 announced a partnership with Microsoft aimed at Intune customers.

UEM for smaller businesses

Kaseya has just announced RMM 2.0 (Remote Monitoring and Management), which integrates its VSA endpoint management software and Traverse advance network monitoring management software. Kaseya has always been strong on supporting enterprises and managed service providers, the latter making UEM available to smaller businesses.

Quest (now no longer part of Dell) has a UEM business unit including its KACE assets with UEM offerings via integrating KACE Cloud MDM with the KACE Systems Management Appliance (SMA). ManageEngine launched Desktop Central in 2005 and in 2012 Mobile Device Management. It says it has had a single UEM console since 2015.

As ever, IBM touts the cognitive capabilities provided by its Watson technology for its MaaS360 UEM offering. Ivanti has built a UEM based around its LANDesk and HEAT assets.

From the MDM/EMM side, MobileIron is one of the leading providers still operating independently from the pack that emerged about a decade ago and now offers UEM. VMware's Workspace ONE UEM is based on its 2014 acquisition of AirWatch. Good Technology was acquired by BlackBerry as it struggled to find a place following the rise of Apple and Android-based iPhones.

Canada-based SOTI has staked a UEM claim with its new SOTI ONE platform. Other players include Matrix42 UEM based on its 2014 acquisition of Silverback, Bejing-based NationSky's NQSky, and Stockholm-based Snow Software.

From the security side have emerged Kaspersky's Endpoint Security for Business and Endpoint Security Cloud for SMBs, which has go-to-market activities with VMware AirWatch and Sophos Mobile.

Moving forward with UEM

Perhaps now is a good time to review endpoint management. Microsoft ended mainstream support for Windows 7 on January 13 2015, and extended support will end on 14 January 2020.

This will mean a major update to user endpoints for many organisations that have not yet moved to Windows 10. The danger of lurking on older versions were well demonstrated by the 2017 WannaCry malware outbreak.

However, this may not just be time to update Windows itself. Perhaps it is also a chance to review the overall usage of user endpoints and, indeed, how all endpoints are managed.

Organisations that have a UEM system in place will be better positioned to provide user choice, but also to address the security of all their endpoints and the cost of managing their ever-growing IT estates. ■