IDC MarketScape

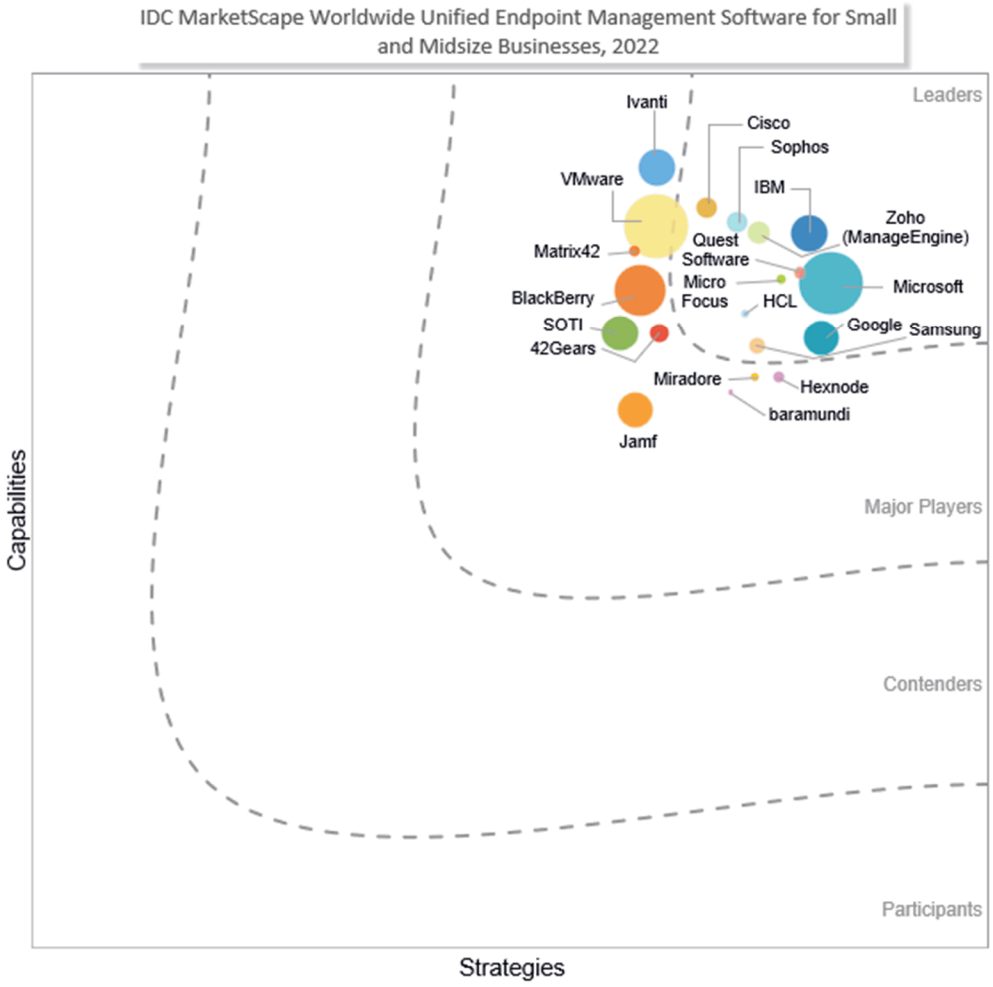
IDC MarketScape: Worldwide Unified Endpoint Management Software for Small and Midsize Businesses 2022 Vendor Assessment

Phil Hochmuth

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Unified Endpoint Management Software for Small and Midsize Businesses Vendor Assessment



Source: IDC, 2022

May 2022, IDC #US48325522

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IDC OPINION

When selecting and deploying unified endpoint management (UEM) software, small and midsize businesses (SMBs) have different requirements, priorities, and trusted supplier sources compared with larger organizations. SMBs typically operate with smaller IT teams, often a few people or a single person responsible for the firm's entire technology estate. This makes the consolidation and integration promise of UEM very appealing — fewer tools for managing, securing, and monitoring more things.

In addition to device endpoint management versatility, SMBs can benefit from bundling UEM tools with adjacent IT products used in the organization's environment — including networking, security, server management, and overall business software platforms. This integration and bundled pricing can sometimes trump the underlying functionality of an UEM product when SMBs are selecting vendors. A best-of-breed UEM may not be the right choice for an organization if it can get an UEM tool, plus a large portion of its overall IT product toolset, from a single vendor.

SMBs also seek technology partners that can integrate with outsourced or managed service providers (SPs), as well as mobile operators/telcos, as these are common channels for SMBs to acquire UEM and mobility technology. Most small businesses tend to source their mobile devices from the mobile carrier they use for service, which makes these carriers important partners for supplying mobility management and, increasingly, UEM tools to SMBs. Similarly, partners can succeed in the UEM market for SMBs if they sell and integrate multiple IT product categories to SMB customers, such as networking, servers, storage, security, and communications platforms. To that end, some key considerations for SMBs looking for UEM partners are:

- Mobile worker front line and remote/hybrid use case requirements for mobility and PC endpoint management
- Support for automation and automated workflows for device deployment, configuration, and provisioning
- The ability to source additional or complementary IT technologies or services from the UEM provider, which are appropriate to the SMB's needs
- Simple workspace IoT rugged device support for SMB-focused use cases — customer kiosks, dedicated/locked-down mobile devices (e.g., apps for delivery staff), and digital signage are some use case examples

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC invited vendors to participate in this assessment based on the following key criteria:

- The vendor has an UEM suite offering device and application management functions for Apple macOS (Mac) PCs and laptops as well as for iOS (iPhone) smartphones and iPadOS (iPad) tablets.
- The vendor has UEM product revenue of $5+ million for calendar year 2021. Revenue was estimated in May 2022 and may differ from forthcoming market share documents.

In addition to the companies profiled in this study, there are a number of other companies in the UEM market. These include Apple, Addigy, Amtel, Citrix, HMD, Kandji, Prey Software, SimpleMDM, Tanium, and Verizon.

ADVICE FOR TECHNOLOGY BUYERS

Buyers of UEM software should look for the following attributes, capabilities, and relevant use case scenario support from vendors under consideration:

- **Enforceable and maintainable device state and functionality.** Transforming a consumer-centric device (e.g., an iPhone or a Google Pixel device) into a locked-down, single-purpose endpoint is relatively simple, but meeting specific industry and use case requirements and security needs is a key consideration for ruggedized and IoT device management platforms.
- **Conditional access controls and policy enforcement triggers.** This is becoming a critical feature of UEM platforms. Conditional access controls what apps, data, or other resources a user can connect to and consume based on an array of factors, such as location (GPS location and network connectivity type) as well as the day, the end-user identity and role, and the state of or health of the device being used (from the standpoint of a jailbroken/rooted device or an operating system [OS] that is out of date).
- **Workspace intelligence and analytics.** With a broad view of endpoint and end-user activity, UEM platforms are becoming a central point of data gathering and analytics on enterprise worker behavior, device, app, and data usage patterns, as well as analysis of software performance and availability. UEM vendors with strong analytics and reporting capabilities around these key metrics will have competitive advantages over vendors not focusing on this area.
- **Baseline mobile endpoint support.** In addition to PC support, core mobility functionality of UEM platforms is in the areas of mobile device management (MDM), MAM, and MCM. Core functional components also include secure PIM, DLP and file access controls restrictions, app wrapping, and SDK capabilities. While UEM platforms are evolving to new use cases and management tasks, these core UEM platform capabilities are still a baseline requirement.
- **Strong portfolio of adjacent and complementary IT products, services, and solutions.** Solutions such as identity, cloud access security brokers (CASBs), IT service management (ITSM), IT asset management, network security, and end-user productivity apps are all important for tight integration with UEM platforms, according to users deploying the technology.
- **A broad set of legacy and modern PC management support functions.** The long tail of PCLM and traditional management requirements means solutions that can address both legacy and modern endpoint management scenarios will have the greatest value to deploying enterprises.
- **Ability to support both mobile and PC form factors.**

VENDOR SUMMARY PROFILES

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

42Gears

42Gears is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Founded in 2009, 42Gears, based in Bangalore, India, has operations worldwide. The company provides a wide range of products, from basic MDM solutions in its product to a full-featured UEM solution in SureMDM. Use cases where devices are deployed in single-app mode or locked down as kiosks are a sweet spot for the vendor. However, 42Gears addresses more than these use cases, with support for secure email, PIM, app wrapping, and all major EMM features. It supports Windows/UEM management as well. It is used in wide-ranging deployments by customers in the retail, hospitality, and logistics industries, where the software is used to provide strong security, app management, and end-user control parameters on commodity Android tablets and smartphones. The SureFox tool is another tool that 42Gears offers for browser kiosk lockdown, which is a component of the SureMDM offering.

42Gears has also greatly expanded its capabilities in supporting desktop operating systems — Windows 10 and Apple macOS, primarily, but also Linux and Chrome OS. The platform can be used to provision, configure and, overall, manage the life cycle of Windows PCs and Macs using modern management, MDM protocol-based controls and APIs. The platform can also manage Linux workstations and servers.

In addition, with a background in supporting Android and IoT-type endpoints, 42Gears is looking to expand its customer use cases to management of augmented reality/virtual reality (AR/VR) headsets, as well as workspace IoT endpoints such as conference room equipment, as well as some crossover into operations technology (OT) for managing devices in industrial and logistical networks and settings.

Strengths

- 42Gears has a strong remote management capability, allowing IT administrators to view the device of an end user to troubleshoot and provide support.
- 42Gears supports a wide range of conditional access scenarios, including location-based policy enforcement, VPN enforcement, and identity/behavior-based access control policies.
- 42Gears UEM uses native platform DLP frameworks (like Android Enterprise and iOS MDM protocol) to segregate personal and work app data (including Microsoft apps), enterprise wipe, secure PIN for container apps, per-app VPN, container data encryption, disable screenshot, and disable copy/paste between work/personal apps.
- 42Gears supports a wide range of device OS types, including PCs (Windows 7 and 10 and macOS), Android, iOS, Linux, and Raspberry Pi and Unix-based devices. This allows the software to address a wide range of mobility, UEM, and IoT use cases. 42Gears' new SureMDM Hub offering helps managed SPs offer device management services to multiple customers from a single deployment of SureMDM (multitenant support), thus lowering their costs and boosting profits.
- 42Gears has strong identity platform integration and support, including SAML, Active Directory, ADFS, Azure AD, Okta, OneLogin, PingOne, and Google Workspace.

Challenges

- While 42Gears has excellent support for Android and iOS platforms, it has limited support for Office 365 on the Windows platform due to limitations from Microsoft on its subscription and license.

- 42Gears has limited support or integration with third-party mobile threat management (MTM) software, identity platforms, or CASB solutions, limiting the enablement of more advanced mobile security and access control scenarios. However, SureMDM can push any third-party MTM client to devices managed by 42Gears' platform.

Consider 42Gears When

Organizations looking to manage every endpoint scenario from a single platform (EMM, UEM, and IoT) should consider 42Gears, especially midsize companies and enterprises looking to consolidate management platforms and create unified management policies.

baramundi

baramundi is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Founded in Augsburg, Germany, in 2002, the device management software company has evolved from providing PCLM and industrial IoT network and management tools to offering a full-featured UEM platform, with support for Android and iOS added in recent years. The company has over 300 employees and serves customers primarily in Europe, as well as North America. The company has over 4,000 customers across a wide range of industries, with a specific focus on industrial/manufacturing.

baramundi Management Suite (BMS) is the single product offering from the company, covering mobile endpoint; BMS runs on a single server in an on-premises deployment scenario to discover, manage, and push policy to mobile devices, PCs, and IoT endpoints.

Policies in BMS can be applied at the user level — such as email groups and physical location — and can also filter down to the device-level configuration. Macrolevel actions, such as terminating an employee, can trigger device-level actions such as device wipe or password deprovisioning. The platform can monitor and enforce policies on a user as well as device-based approach. Users, via an Active Directory integration, can be associated with multiple devices — mobiles and PCs. The company offers a self-service portal, with the ability to support IT administrators in terms of self-service, as well as an end-user-facing self-service portal for employees enrolled on the platform.

Strengths

- baramundi has a very low cost-per-device price point compared with other vendors, especially among those focused on SMB customers.
- baramundi has a strong management story for off-network devices, or endpoints not connected to an on-premises/behind-firewall or VPN network.

Challenges

- The company does not currently support key device auto-enrollment/provisioning standards, such as Android Zero Touch (although the company plans to offer this in its 2022 road map).
- The platform is only available as an on-premises product. No cloud-based version of the product is currently on the road map. (However, the software can be run as a virtual machine hosted in a cloud environment.)
- There is limited reporting and analytics capabilities, such as Windows/macOS application performance monitoring, auditing of data access, and overall app performance capabilities.

Consider baramundi When

Firms should consider baramundi as a competitive/comparative EMM/UEM and workspace IoT platform for endpoint and connected device management.

BlackBerry

BlackBerry is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

BlackBerry is a Canadian endpoint device management and security software vendor based in Waterloo, Ontario. The former smartphone and devices manufacturer now focuses on UEM software, as an evolution of its BlackBerry Enterprise Server platform, integrated with technology acquired from EMM/MDM vendor Good Technology. The current offering, BlackBerry UEM, covers the four major operating systems — Windows, macOS, iOS, and Android — from a management, deployment, and maintenance perspective.

BlackBerry as a company has created two business units to focus on cybersecurity and IoT, respectively. The BlackBerry UEM product falls under the cybersecurity group, along with technology acquired in the 2019 buyout of cybersecurity software vendor Cylance. BlackBerry has always been a pioneering vendor in mobile security (especially with regard to data-at-rest and data-in-transit security for connected wireless devices). Since the acquisition of Cylance, BlackBerry has put even more emphasis on its position as a cybersecurity software vendor, with products now including endpoint security software, endpoint detection and response, extended detection and response, threat intelligence and analytics, and mobile security. The UEM product ties closely to these offerings such as endpoint security and threat analytics. This allows BlackBerry UEM to incorporate security intelligence data and telemetry into how endpoints are managed, configured, and monitored. A major use case BlackBerry is promoting along this line is continuous authentication and access control. By closely monitoring the security state of all endpoints — both mobile and PC — BlackBerry UEM can disconnect or quarantine devices based on their security and risk posture.

On the Mac front, BlackBerry has increased support for Apple device and identity management features, including multiuser iPadOS functionality, as well integrating Managed Apple ID support for allowing end users to have both personal and work-related apps, as well as work-managed apps and data on a personal iPhone.

In 2021, BlackBerry released its BlackBerry Gateway offering, a zero trust network access solution that complements and integrates with the UEM product, allowing for remote endpoint access to firewalled corporate IT resources, as well as cloud-based apps and data without a VPN or cloud proxy overlay technology. The solution uses BlackBerry's Cylance-based AI capabilities for monitoring ongoing network and app activity of Gateway and can enforce remediations and restrictions on devices if anomalous or suspicious activity is detected on connected devices.

BlackBerry also has a large development community of customers that created customized and specialized mobile apps on the BlackBerry Dynamics platform. BlackBerry provides users with mobile app development, containerization, and wrapping functions that can insert increased security and threat detection features into off-the-shelf mobile apps.

Strengths

- BlackBerry's UEM offering meets a wide range of government and industry certifications around security and compliance, including FedRAMP, FIPS 140-2, NIAP Common Criteria, and PCI-DSS, among several others. The UEM product is on the approved vendor listings for a number of U.S. and foreign government organizations as well.
- BlackBerry's extensive cybersecurity products portfolio, and the AI technology behind its threat detection and remediation capabilities, provides a powerful tie-in to the UEM solution, especially for use cases requiring continuous authentication and security health checks of endpoint devices accessing corporate data and apps.
- BlackBerry's mobile threat management technology integrates with the UEM product to provide a strong management/security endpoint offering for smartphones, tablets, and IoT devices running mobile-centric OSs such as Android.
- BlackBerry UEM integrates tightly with the vendor's critical event notification and management SaaS platforms, BlackBerry Alert and BlackBerry AtHoc. This includes pushing specialized, deterministic messages to endpoint devices, as well as integrating with device access control settings and policies to adapt to emergency situations.

Challenges

- BlackBerry customers interviewed for this study said that while the highly secure functionality of BlackBerry UEM is a strong benefit, the technology is somewhat inflexible and costly for meeting some of the more generalized use cases around mobile computing and data access.
- BlackBerry lacks support for Linux and Tizen, which could limit the vendor's inclusion in some workspace IoT use cases and deployment scenarios. However, BlackBerry has strong IoT technology and market presence with its QNX real-time operating system in deployments such as automotive and industrial use cases. However, for workspace IoT solutions (managing conference room equipment, AR/VR equipment, etc.), BlackBerry has fewer support capabilities than some of its competitors.

Consider BlackBerry When

Consider BlackBerry for high-security use cases or scenarios where regulatory compliance and special certifications are important requirements, especially for bring-your-own-device deployments that can leverage BlackBerry's secure productivity apps. Also consider BlackBerry UEM for potential vendor consolidation and product integration with regard to the vendor's BlackBerry endpoint security and threat detection products. BlackBerry's capabilities around mobile data protection and security also make it a strong consideration for supporting extensive BYOD deployments.

Cisco

Cisco is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Cisco, and its Meraki business unit and product line, is one of the largest networking, cloud, and IT product vendors in the world, and one of the companies that built the internet as it is today. Cisco's UEM solution sits in its Meraki business unit, focused on converged, integrated network infrastructure targeted at enterprises as well as SMBs.

Simplification is the overriding strategy and approach for endpoint management, with a specific tie-in to the underlying Meraki network infrastructure. This tight coupling of endpoint management with network connectivity is Cisco's differentiation with Meraki Systems Manager.

New functionality added in the past 12 months has focused around the device enrollment and end-user onboarding functions. Multifactor enrollment was added to support SAML integration, which helps support cloud identity platforms. Meraki Systems Manager also integrates with Cisco's DUO mobile identity and security product, brokering MFA enrollment.

From an Android perspective, frontline worker is another area of focus, including definitive support for Android app life-cycle management, including Android Google Play EMM API, to manage high-priority updates, allowing to ignore device state in deploying apps, as well as postponing app and software updates (useful to test apps before deploying on new iterations of the Android OS).

Cisco has gone to lengths to help integrate more pieces of the Cisco and Meraki product portfolio with the Systems Manager platform. This positions Systems Manager to be a foundational product for enabling and managing Cisco's entire "Zero Trust" architecture.

Auto-provisioning VPN and providing lightweight network access control (NAC) allow policy to be deployed directly on devices connecting to a Meraki network. Key use case integrations include quick setup of secure Wi-Fi networks with endpoint configurations. Cisco's Identity Services Engine (ISE), AnyConnect VPN platform, and Umbrella secure DNS functionality also can integrate with Cisco Meraki Systems Manager.

Strengths

- The broad portfolio of security products that Cisco offers and the fact that these products can integrate with Systems Manager is a strong differentiator for the vendor. Integrating UEM software with security technologies (identity, network security, and other products) is a specific strength of Cisco as the company's product lines in these areas are far-reaching and well established.
- Cisco also introduced its Trusted Access technology on its Wi-Fi product (MR) network infrastructure where Systems Manager is running. This allows for the management and control of endpoints connecting to the wireless network that may or may not be fully managed by MDM or UEM enrollment.
- Trusted Access applies to the action of connecting to the network; the product can take devices and apply networking rules via the back-end NAC infrastructure that Cisco provides.
- From an Apple perspective, Meraki Systems Manager has added deeper integration with Apple Education features. This includes the deployment of multiuser iPads (where multiple users can log in to an iPad with different IDs). Temporary guest session for frontline workers is another use case Cisco is targeting with this function.

Challenges

- Deeper integrations with other Cisco products, such as API-based integration with Cisco ISE, are still on the road map.
- While Cisco's Meraki Systems Manager provides a broad range of strong access control device management and enhanced security functionality integrated into the UEM platform, users must be deep into a Cisco networking and security installed base. Non-Cisco environments or enterprises with mixed environments for infrastructure will not be able take advantage of integration features with Systems Manager.

Consider Cisco When

Consider Cisco's Meraki Systems Manager for UEM deployments where tight integration into the network and network security infrastructure is a high priority. Both large organizations and SMBs looking to consolidate IT infrastructure and software vendors should also consider Cisco, especially if they are already using Cisco/Meraki infrastructure.

Google

Google is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Google, founded in 1998 as an internet search engine company, has evolved into an internet technology giant and wide-reaching enterprise cloud software vendor, serving SMBs and enterprises. Google Endpoint Management is a component of the larger Google Workspace suite and integrates tightly with Google Cloud Identity – an integrated component of Google Workspace – but also available as a stand-alone product. While Google Endpoint Manager targets endpoints running Google Workspace services, it also extends to other cloud-based apps and resources – devices with G Suite/Cloud Identity accounts – with capabilities such as account wipe, password enforcement app inventory, and other basic functions. The platform can provide these features with "agentless" scenarios – where only the presence of Google apps or Chrome browser is sufficient. Deeper, more sophisticated actions can be performed on fully managed devices, with stronger enforcement policies, conditional access rules, and other advanced features.

Strengths

- Google added stronger Windows 10 capabilities to its UEM offering in 2020, including an agent-based option for Windows 10 management, allowing for deeper and more sophisticated management and provisioning scenarios for Windows devices used with Google Workspace, including integration of local and Google admin accounts on Windows devices and auto-provisioning of setup and services.
- Google Endpoint Manager has strong security and management functions around Workspace apps, including cross-platform mobile/cloud apps management. It has strong data protection capabilities for securing sensitive data accessed and used by Google Workspace apps.
- Google's BeyondCorp data and identity-based security approach and principles are recognized widely as the future of security for cloud-centric enterprises and companies. Google Endpoint Management integrates these concepts of identity-based access controls, and security policies tied to data and apps, as opposed to physical devices and their location or network attachment.
- Google's strong single sign-on and federated ID capabilities allow Google Endpoint Management-managed endpoints to connect to a range of third-party applications and cloud platforms supported by Google Cloud ID. Strong support for FIDO and two-factor authentication functions round out the strong access control story for Google-based device management.
- Google has broad support and integration for cloud security and authentication tools, including third-party ID platforms (i.e., Okta, Ping, Azure AD) and cloud security platforms such as Bitglass, Cisco, Microsoft Cloud App Security, Netskope, and Zscaler.

Challenges

- Google Endpoint Management does not support key Apple Business Manager functions, such as device deployment and app volume purchasing functions. Apple Support for these frameworks as well as Apple's new User Provisioning capabilities (for advanced BYOD iOS device management) are slated for support in 2022. While macOS management is supported in terms of G Suite apps and Google Cloud ID on Macs, full agent-based support for macOS is not currently available, but it is on the company's long-term road map.
- While Google owns/maintains the overall Android mobile OS development and life cycle, Google Endpoint Manager does not support some of the Android Enterprise-specific features for specific use cases, such as Android single-app mode, dedicated device profile, or shared device support.
- Google Endpoint Manager does not support workspace IoT or any other extensible IoT endpoint management technologies. The platform is primarily focused on managing knowledge worker and traditional end-user computing management scenarios (with specific focus on Google Workspace apps).
- While it has strong enterprise cloud security and ID integrations, Google Endpoint Manager lacks as broad an integration story around enterprise system management tools such as ITSM and security information and event management (SIEM) software.

Consider Google When

Organizations standardized on Google Workspace productivity apps should consider Google Endpoint Management broadly, especially if their environments are primarily Windows-based, with a mix of iOS and Android mobile devices. SMBs (as well as businesses deploying Chrome OS) should also consider Google for Google Endpoint Management.

HCL

HCL is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

HCL is a global IT software and services firm based in India, with customers and subsidiaries around the world. The company's UEM solution is based on its BigFix platform — a long-used IT management, configuration, and maintenance platform across PCs and servers. BigFix, which originated in IBM, was spun off to HCL in 2019, along with several other enterprise IT product lines. In 2021, HCL launched iOS and Android device support for BigFix, putting the product squarely in the UEM category.

BigFix has extensive Windows PC and macOS management capabilities, with a strong focus on patch management, automation, software life-cycle maintenance, and software threat and vulnerability remediation. An agent-based system, BigFix can perform extensive device inventorying functions (hardware and software installed) and can configure granular policies on endpoint PCs, Macs, and servers. From this, HCL BigFix is a strong tool for helping end users with compliance and regulatory requirements around endpoint security and management (e.g., PCI-DSS, NIST, CIS, and DESUS). BigFix is also known for its ability to manage large-scale deployments of endpoints, with upward of half a million endpoints and more in some of its largest deployments. BigFix also supports robust remote monitoring and management functions for accessing users' PC environments and helping troubleshoot issues in real time on a system.

Automation and integration are key features of BigFix. With the ability to widely and quickly update software and patches, the platform integrates with key threat and vulnerability detection platforms,

such as Qualys and Tenable. BigFix also integrates with ServiceNow, Rapid7, Forescout, Aruba, Malwarebytes, IBM Resilient, IBM QRadar, Nutanix, VMware, Intel vPro, Google Cloud, Azure, and AWS.

While BigFix was an acquired technology, the customer experience with the product post-IBM spin-off has been positive overall. Since its spin-off from IBM, the BigFix product and organization has grown and expanded under HCL. Several BigFix customers interviewed for this study said they saw an increase in new feature development and feature requests, responsiveness to support and integration issues, and an overall higher level of customer satisfaction with the platform over the past two years.

Strengths

- Software patching and operating system patches and updates are a particular strength for BigFix. The platform can support a wide range of automations for ensuring endpoint apps and device software are up to date and compliant. The platform can also interact with other security and monitoring platforms to quickly update vulnerable or at-risk endpoints.
- BigFix UEM has strong reporting capabilities, with the ability to create a diverse range of deeply detailed reports and repeatable report templates on endpoint device's state, history, compliance status, and other attributes. Data can be exported to platforms such as Power BI and Tableau for analysis.
- HCL is among a few UEM vendors that have strong server (Windows and Linux) device management capabilities built into the UEM platform overall. While not an endpoint management function required by most end-user computing teams, server management as an additional capability is valuable for organizations looking to consolidate IT roles and tools. Server management also gives HCL UEM an advantage in deployments on VMware and Nutanix, and IoT devices based on Windows 10/Windows 11 and Raspberry Pi are also strong features targeting SMBs.

Challenges

- With the addition of iOS and Android in 2021, BigFix became a full UEM platform with the ability to address all four major endpoint OSs (Windows, macOS, iOS, and Android) with a modern management (agentless) approach. While its mobile OS management feature set is strong out of the gate, support for these technologies is new for BigFix, while some of its competitors have half a decade or more of history in supporting mobile devices and app management.
- BigFix is primarily an on-premises software platform and is not yet delivered as native SaaS; however, HCL and many partners offer BigFix as a hosted service. This is a challenge for the vendor in addressing customers looking for a purely cloud-based or SaaS-delivered UEM product. (The majority of the UEM market is now cloud based.)

Consider HCL When

Consider HCL BigFix as an UEM platform for enterprise deployments where strong patch management, discovery, endpoint state inventory, and automation are key requirements. Customers with another UEM/MDM product in place should evaluate BigFix as a possible consolidation opportunity for mobile device management. SMBs should also consider BigFix as a complete, unified IT management and configuration platform across PCs, Macs, mobile devices, and a broad array of server operating systems (with over 100 variants of server OSs supported).

Hexnode

Hexnode is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Hexnode is the enterprise software division of the San Francisco–based Mitsogo Inc., founded in 2013, and currently has approximately 300 employees. Its UEM product, Hexnode UEM, is a cloud-based product. The company originally focused on SMBs and Apple-only devices, but it has expanded to enterprise-scale customers (5,000+ customers) with worldwide customer base. Currently, Hexnode supports iOS, macOS, iPadOS, tvOS, Windows, Android, Android TV, and Amazon Fire OS. While the product has customers globally, more than 50% of its customers are in the United States.

Hexnode UEM supports Windows 10, Apple macOS, iOS, and Apple TV devices, as well as all current Android versions (including Android Enterprise technology). Hexnode supports software updating, configuration management, app delivery, and policy enforcement on all devices running these four major operating systems. Hexnode provides a browser-based portal view where administrators can see device status and state. The portal can also be used to launch a remote view window for seeing an end user's screen on Windows, Mac, iOS, and Android. Hexnode supports a range of kiosk support options, including single-app and multiapp kiosk across iOS, Android, and Windows 10. Web apps are not supported on Windows 10 devices, but native apps are supported in Windows. Single app for Apple TVs is also supported, such as for conference room sharing or single-app access in Apple TV. IT also supports deployment of Android devices in digital signage use cases, where only certain content or images are displayed.

On mobile, Hexnode can monitor mobile data usage on iOS and Android devices, as well as managing and enforcing policies for Wi-Fi data usage on Android only. Hexnode can also support out-of-the-box enrollment of iOS and Android devices with Apple Business Manager and Android Enterprise zero-touch support. The product supports Apple Business Manager/VPP for app deployment and management as well as Android Enterprise Managed Google Play.

On Mac management, Business Manager integration allows for admin accounts to be created and managed by Hexnode. App installation by end users can also be restricted, requiring all apps to be automatically delivered via the Mac App Store. For security agents on Mac, Hexnode can support system and kernel extensions required for support. Macs can also domain-join devices for Active Directory to force directory-based access control for Mac users. OS updates can be automated via Hexnode for macOS and control access of external media and storage on managed devices.

On the Windows side, Hexnode has an endpoint client for management, which allows for finer-grained management function supporting a comanagement function for Windows devices. Hexnode can also support Windows MDM protocol-based management of Windows.

From an IoT perspective, Hexnode can support Android smart TVs, Amazon Fire tablets, and Apple TVs. However, the platform does not currently support Linux, which could limit the platform for more extensive workspace IoT device deployments that often rely on Linux-based endpoints such as Raspberry Pi devices and many consumer IoT electronic interfaces.

Hexnode sells the majority of its product directly over the web but has limited partnerships with resellers and mobile operators.

Strengths

- Hexnode has strong automation capabilities to push whole endpoint configuration profiles, apps, and policies to large groups of devices. The automation can be based on what region the devices are located, or what organization or team the devices belong to.
- The product integrates with major identity platforms such as Microsoft Active Directory, Azure Active Directory, Okta, and Google Cloud Identity.
- Third-party app patching is supported across all software platforms, so automated third-party apps are pushed to endpoints when new versions are available on the Apple and Google Play stores.
- Hexnode can enforce or limit encryption on Mac endpoints. Screen savers can also be controlled and managed via Hexnode.

Challenges

- The product currently does not support automated patching for Windows 10. It currently relies on custom scripts to push OS updates and other patches for Windows devices. Automated patching is supported for Mac, iOS, and Android, and Win10 support is planned for release in 2022.
- Hexnode's licensing model is device based, requiring a user with multiple devices to have multiple per-month device licenses for management. This can be cumbersome and costly in some instances where large numbers of end users have multiple managed devices (e.g., a Windows laptop, iPhone, and Android tablet).
- Hexnode's remote control supports all Android devices. The company plans to add Mac and Windows endpoint control for end-user support in 2022.
- Hexnode has several strong integration features with large identity providers such as Microsoft, Okta, and Google and also with Jira and Zendesk for IT ticketing. However, the product does not support integrations with enterprise service or asset management platforms such as ServiceNow, or security integrations. (The product does not currently integrate or partner with any third-party endpoint security, mobile threat management, or SIEM platform providers.)

Consider Hexnode When

SMBs and Apple-centric firms should consider Hexnode UEM as an all-inclusive endpoint device management platform. Large enterprises with heavy Mac usage, as well as firms with large, distributed workforces and SaaS requirements should also look at Hexnode.

IBM

IBM is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

IBM Security MaaS360 with Watson is a cloud-based UEM product with strong adoption among both larger enterprise and small/midsize businesses. MaaS360 is part of the larger IBM Security business unit of the software company and has strong ties to other adjacent IBM Security solutions, ranging from identity, data, endpoints, and cloud security as well as analytics. As the name implies, the UEM product has strong AI- and cloud-based intelligence features through incorporation of the IBM Watson cloud AI platform.

MaaS360 covers the four major end-user computing operating systems: Windows, macOS, iOS, and Android, as well as capabilities for extending management and policy enforcement to Chrome devices. The platform's flexibility suits it for use cases including general mobility management, cloud-based PC and Mac management, and more specialized device management scenarios such as frontline device, ruggedized device, and some IoT endpoint management.

As part of IBM's Security business unit, MaaS360 has multiple feature integrations with several IBM Security platforms, including QRadar threat intelligence; IBM's Verify platform and Guardium vulnerability and data security technologies also integrate with MaaS360.

Strengths

- IBM has strengthened its ability to manage Windows devices with more granular policies, such as GPO-based configurations and policy enforcements. This can allow organizations to migrate more easily from on-premises PC management tools (e.g., script/agent-based tools) to cloud-based UEM and modern management.
- MaaS360 can support macOS management functions including software distribution, identity integration, macOS app patching, and Mac configuration management and policy enforcement.
- MaaS360 has broad support for critical PC and mobile endpoint management features across four major operating systems as well as extensive Chrome OS/Chromebook management support. All the major zero-touch deployment and technologies are supported (Windows Autopilot, Apple DEP, Android zero-touch, and Knox Mobile Enrollment).
- MaaS360 has strong carrier partnerships, selling through mobile operators such as AT&T, Verizon, and T-Mobile in the United States and Vodafone, Orange, Singtel, and Telefónica in other regions. This greatly expands MaaS360's potential customer base across enterprise and SMBs.
- MaaS360 can be used to manage IoT and ruggedized devices such as Linux and Raspberry Pi and rugged devices such as Zebra, Android Things, and Windows IoT. Apple TVs and Apple Watches can also be controlled by the platform.

Challenges

- While very strong in security analytics, IBM has fewer analytics capabilities targeting end-user satisfaction and experience scenarios and use cases. This is an increasingly important area to support in UEM as the technology becomes a more integrated component of larger intelligent digital workspace systems.
- While IBM has strong security, identity, and cloud platform integration opportunities with MaaS360, the vendor's overall portfolio is less end-user-computing centric than some competitors.

Consider IBM When

Consider IBM for most UEM use case scenarios, especially where "cloud first" is a key consideration. Also consider MaaS360 for specialized deployments such as single-use device, ruggedized device, and frontline device workspace scenarios.

Ivanti

Ivanti is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Ivanti UEM is a mobile/PC management software platform that includes device management, patch management, and identity integrations and tie-ins to the company's security technologies. Ivanti has a large installed base of PC life-cycle management users (e.g., LANDESK), which provides a large base to deploy and migrate customers from traditional to modern management. The company also has a large install base of mobile device management users (e.g., MobileIron). The Ivanti Neurons Platform is another aspect that adds more dynamic capabilities to Ivanti's UEM offering. The software platform for IT operations automation can extend to advanced endpoint device management workflows, allowing for automated patch management, vulnerability monitoring, and remediation. Neurons also extend into the IoT device management space, allowing for IT processes for connected things and nontraditional endpoints and systems to come into the UEM/Neurons fold. The vendor also brings a range of use case-based Neurons workflows, such as human resources, facilities, and PMM, that incorporate endpoint device management and provisioning with broader end-user enablement capabilities.

From a strategy perspective, Ivanti has done a good job integrating the combination of technologies from the LANDESK and HEAT PCLM products with MobileIron EMM/UEM and Pulse Secure remote access and workspace security technologies. The 2021 acquisition of Cherwell Software, in the ITMS space, also gives the company another strong cross-selling and integration opportunities.

Strengths

- Ivanti provides management and security capabilities across a wide range of devices including iOS, Android, Windows, macOS, Chrome OS, Linux, and IoT. In addition, the company provides support for a wide range of use cases, including BYOD, corporate-owned frontline workers, and other vertical-specific use cases.
- Ivanti has strong support for both Windows and macOS endpoints, at a very detailed level, including OS and third-party patch updating, vulnerability management, hardware/software inventorying, application delivery, and provisioning as well as support for legacy management functions and features, such as device imaging (both Windows and Mac), GPO management support (Windows), printer management and setup (Windows/macOS), and modern and legacy app distribution for Macs (DMG file distribution and managed Mac App Store support).
- Ivanti also provides comprehensive mobile device management capabilities for iOS and Android devices. Capabilities include zero-touch onboarding, app containerization, secure productivity, and integrated mobile threat detection and antiphishing.
- Ivanti is the only vendor that provides end-user support, security, and technology operations product portfolios among UEM vendors in the market. Adjacencies in ITSM and IT asset management allow Ivanti to provide a Digital End-user Experience (DEX) Management score, which is derived from experience metrics across device, security, and IT service management.
- Ivanti's peer-to-peer, multicast patch and software updating technology can deliver large software updating payloads to multiple devices without overconsuming bandwidth, which is critical for hybrid and remote workers.

Challenges

- While Ivanti has gone a long way to integrate and provide a road map for how its acquired, and native, technologies will integrate, some customers IDC spoke with are still learning of the broader product strategy and see Ivanti from the context of specific products.
- Some Ivanti customers IDC spoke with for this study said they had communication challenges with regard to providing product feedback and new feature suggestions. Customers felt this was somewhat related to the ongoing integrations of the vendor's recent acquisitions.

Consider Ivanti When

Businesses looking to converge most end-user computing device management, security, and service desk support functions should consider Ivanti as a potential single-source vendor. Enterprises should also consider Ivanti UEM if integrations with zero trust security platforms, IT asset management, patch, vulnerability detection, and IT service management are important.

Jamf

Jamf is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Founded in 2002, Jamf evolved its technology from the group of systems administrators at the University of Wisconsin-Eau Claire who had a large Apple desktop environment to manage. The team productized its technology and released its Casper Suite primarily supporting educational deployments of Macs but also enterprise and business environments. Through the 2000s and into the 2010s, the company grew in revenue and devices under management as Mac's popularity grew in business, particularly in the high-tech industry, as well as its traditional strongholds in education and creative industries. As Apple introduced new devices, most notably the iPhone, Jamf expanded into mobile and tablet device management, with a focus on offering an integrated, Apple ecosystem-centric approach to cross-platform and cross-form factor endpoint management.

Many other products on the market can manage Apple devices. Although being closely aligned to growth of Apple devices has benefited Jamf, the UEM vendor's success is not solely tied to Apple's success. Jamf differentiates by offering extensive management capabilities, especially for macOS devices, with an agent-based management framework, which can drill down deep into Mac systems and provide extensive capabilities for configuring, managing, patching, and securing Macs for business use. The company has also selectively plucked emerging and popular Apple-centric management and security software start-ups with an integration strategy focused on adding incremental functions and capabilities.

Jamf is also an UEM company, in that its offerings can manage endpoint devices with form factors that are either PC or mobile — laptops/desktops and smartphones/tablets. While used as a specialty tool in many instances to manage Macs in larger environments with other endpoint device types, the company offers benefits around UEM when managing all-Apple endpoint environments. This could include coordinated provisioning and deployment of apps to users' Macs and iPhones, application of policies across multiple device types, and deprovisioning and other security functions that could affect a single corporate user's many Apple devices.

Strengths

- One aspect of Jamf's overall strategy and successful approach has been how quickly the company can react to Apple's extremely guarded and much anticipated operating system release cycles. Jamf has established a strong reputation in the device management market for supporting new versions of macOS (the major title releases — "Catalina," "Big Sur," and "Monterey") as well as major and minor ("dot") releases to the iOS and iPad mobile/tablet operating systems.
- In July 2021, Jamf acquired Wandera, a United States-based mobile threat management, zero trust network access, and mobile technology management and policy enforcement software vendor. Wandera software can act as a monitoring and policy enforcement tool for mobile data usage, as well as a zero trust network access control platform overall for enterprise

connectivity and modern endpoint security and monitoring. With Wandera technology, Jamf gains security and threat detection capabilities for Android and Windows 10 (as well as iOS), extending its endpoint capabilities beyond the Apple ecosystem.

Challenges

- Jamf's principle to only manage Apple devices has proven to be a winning strategy, given the vendor's financial performance and customer growth. However, it remains to be seen, long term, how well the vendor will compete with larger enterprise UEM vendors that support four or more endpoint device OSs (Windows, macOS, iOS/iPadOS, and Android) as opposed to only two, as is the case with Jamf.
- While Jamf has a large SMB and midmarket installed base, Apple-focused vendors such as Addigy, Hexnode, and Kandji have aggressively targeted the midmarket and SMB segments, where cloud-based UEM services churn is high. Jamf risks losing mindshare, and managed device market share, to these start-ups, especially as their customer bases grow from midmarket/SMB to larger enterprise-level customers.
- While doing one thing very well (Apple device management), Apple-exclusive enterprises are the minority; most firms have multiple operating systems. Jamf is not able to address these organizations or multi-OS use cases as effectively as other UEM competitors.

Consider Jamf When

Consider Jamf for Mac and iPhone/iPad device management if your organization uses Apple devices exclusively. Also, organizations with large Mac deployments, in addition to other endpoint types, should consider Jamf as a specialty-use endpoint management tool, alongside other UEM and client endpoint management tools used to manage non-Apple technology.

Matrix42

Matrix42 is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Based in Frankfurt, Germany, Matrix42 is a provider of EMM and platforms targeting a wide range of endpoint management use cases, with a focus on UEM. The 24-year-old company started in Windows system management and has expanded to EMM/MDM and UEM solutions. It now combines its previously separate Emperium (PCLM) and Silverback (MDM) products into a suite called Matrix42 UEM. The company also offers several key EUC and security-focused products that tie into its UEM offering. Matrix42's IT asset management and service desk products can integrate with UEM to trigger help desk tickets from mobile devices, as well as provision and track devices, apps, software licenses, and other assets associated with an employee or a team. Matrix42 also offers a Windows-based endpoint security product, which can be deployed via UEM and integrates into the UEM dashboard and management console.

Beyond UEM and integrating disparate IT management products, Matrix42 has a larger workspace management strategy, focusing on employee engagement (with measurement/tracking for end-user satisfaction), and AI-based workflow automation (automatically remediating issues with device software, apps, etc.) as well as quick-app and user workflow creation capabilities.

Strengths

- Matrix42's UEM product has strong support for management features and policy deployment across four major operating systems (Android, iOS, macOS, and Windows) as well as support for the emerging Chrome OS platform.
- The UEM dashboard combines data and views across all EUC device types and can also push configuration changes, configuration/policy changes, and apps (mobile and desktop) to all endpoint types.
- Matrix42's broader software portfolio can help smaller IT teams converge multiple IT tasks and systems into a single buying center and integrated solution (e.g., teams responsible for all aspects of EUC, including service desk, security, and asset management).

Challenges

- Matrix42 has limited support for third-party MTM solutions compared with larger vendors. MTM support is an increasingly important factor in EMM deployments according to customers interviewed for this IDC MarketScape. Support for third-party CASB and identity platforms was also more limited.
- Matrix42 has limited distribution channels and partners outside of Central and Eastern Europe, where it is based. While very strong in this geography, this limits the company as a regional player with difficulty to support global enterprises.

Consider Matrix42 When

Consider Matrix42 for advanced UEM deployments in midsize to small enterprises, especially among organizations that have already converged PC and mobility management and support teams. Organizations based in the European Union (EU), or with large regional operations in this area, should also put Matrix42 on a short list of vendors for consideration.

Micro Focus

Micro Focus is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Micro Focus is a United Kingdom-based enterprise IT management and security software vendor with a large enterprise software product portfolio. ZENworks UEM is an evolution of the company's ZENworks product line of PCLM, ITSM, identity, security, and other management software (originally created by Novell, which Micro Focus previously acquired).

ZENworks has a strong analytics story. The company acquired Interset, which made user behavior analytics software. Micro Focus combines this with its device-level logs and data to provide analytics on end-user behavior combined with endpoint device configuration and asset information. ZENworks integrates with Android Enterprise as well as Microsoft Graph API for Office 365 app policy enforcement and integration. It also supports tvOS for Apple TV deployments where the devices are configured and managed centrally for single-use deployments (conference room presentations, interactive/dynamic digital signage, etc.).

ZENworks has a wide range of complementary management and reporting software products, including ZENworks Asset Management (can be tied to contracts, allowing for monitoring of software usage for billing purposes) as well as ZENworks Service Desk, an ITIL-based IT service desk solution that can integrate with ZENworks UEM. ZENworks Endpoint Security Management is another tool in the portfolio relevant to EMM/UEM with adjacent integration capabilities that protect Windows devices,

including antimalware/antivirus, low-level firewall capabilities, app blacklisting, and VPN enforcement (i.e., for public WLAN access point connections and fixed and removable drive encryption). Other adjacent software platforms that integrate with ZENworks in the Micro Focus portfolio include NetIQ eDirectory for IAM and ArcSight — the SIEM platform formerly owned by HPE's software division, which spun off and merged with Micro Focus in 2017.

Strengths

- Micro Focus supports a broad range of Windows policy enforcement capabilities with an on-device agent that can offer deeper levels of control and management as opposed to over-the-air UEM Windows management tools that rely only on the MDM protocol for modern PC management.
- Micro Focus can deploy a sandboxed endpoint environment to managed endpoints in the form of an OS container, which can help prevent against data loss on endpoints, while limiting what types of files and apps can be accessed and executed on the endpoint.
- ZENworks UEM integrates tightly with Micro Focus' other IT products such as data protection, security, and identity platforms, making it a strong tool in a multiproduct Micro Focus environment.
- ZENworks can manage devices efficiently in remote locations by detecting the location of the end user (via the UEM desktop agent) and provision the right set of applications and restrictions, depending on where the worker is (i.e., in the office, at home, or traveling). This can be coupled with remote management capabilities to help troubleshoot devices.

Challenges

- ZENworks UEM does not support Apple macOS device enrollments with automation provisioning, app distribution, or policy setup, although this is in the vendor's near-term road map over the next 12 months.
- Some Micro Focus customers IDC interviewed for this study said that they found the ZENworks UEM platform somewhat cumbersome to use in terms of setting up reports for device status, inventorying, and monitoring. Data out of the reports was good, once set up, but the templating setup method was difficult, users said.

Consider Micro Focus When

IT teams operating with small or minimal staff should consider ZENworks UEM. SMBs are also prime candidates to consider the platform, as it can incorporate multiple IT functions into a single product. Larger firms using multiple Micro Focus products (such as identity, data protection, or security products) should also consider ZENworks UEM from a single vendor-management and product integration perspective.

Microsoft

Microsoft is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Based in Redmond, Washington, Microsoft is among the world's largest software vendors and technology companies with a vast product portfolio spanning enterprise, consumer, and vertical markets. In the UEM market, Microsoft Endpoint Manager is the main product offering. The umbrella product brand encompasses the vendor's on-premises System Center Configuration Manager (SCCM, or ConfigMgr), as well as the Microsoft Intune cloud-based PCs (Windows and Mac devices) and mobile device management platform. With these two components, Microsoft offers a broad set of UEM

use cases and scenarios for managing PCs and mobile devices. This could include managing a fleet of Windows PCs completely on premises, with Active Directory domain-joined functionality, as well as managing cloud-based PCs, and deploying software to endpoints via modern management (MDM) protocols and services.

Microsoft Endpoint Manager can also address hybrid or migrating use cases where customers are moving from on premises to modern management but require tools to address devices in both environments. For example, MEM "tenant attach" capability allows on-premises PCs to be managed with a cloud-based console and to be viewed in a single portal or as mobile devices and cloud-managed endpoints. Integration is a key aspect of the Microsoft Endpoint Manager offering, and the product ties into a wide range of other tools from the vendor, including Office 365 apps, Teams, and OneDrive as well as Microsoft security products including Microsoft Defender for Endpoint (endpoint security) and Microsoft Sentinel (security information and event management).

Analytics and end-user experience are major focus areas of Microsoft Endpoint Manager. Endpoint Analytics is a built-in capability of Endpoint Manager, allowing IT admins to view detailed data and analytics on how end users are interacting and experiencing overall endpoint device and app usage. This could include viewing, and remediating, devices with slow boot-up times, flagging apps that frequently crash or take too long to launch, or diagnosing network or remote access capabilities.

From a licensing and cost perspective, Microsoft Intune license for Endpoint Manager is bundled into several widely used enterprise licensing programs that Microsoft offers around the Microsoft 365 product line and licensing scheme. Customers with E3 and E5 Microsoft 365 licenses can activate modern management of endpoint devices within their existing licensing scheme at no additional cost. This is a compelling consideration for many large enterprises that are already licensing Microsoft technology at a large scale.

Strengths

- Microsoft has added a range of updates and improvements in its Mac device management functionality for macOS endpoints managed by MEM. This includes the ability to apply granular policies to Mac software distribution and deployments, broader support for macOS device configuration profiles, and user-based policy enforcement customization.
- MEM is strong on frontline/rugged device management, which includes devices running Windows IoT and Microsoft's HoloLens AR hardware, as well as vertically focused endpoints such as Zebra.
- The Microsoft 365 product bundling is compelling for small and midsize businesses, by combining PC OS, productivity/collaboration, and management software in a single offering. For midsize firms, or businesses with lean/limited IT staff and resources, comanagement with ConfigMgr can converge Microsoft Windows 10 and Windows Server management into a single console and management environment.
- Microsoft 365 Lighthouse, an administrative portal the company has developed for supporting managed service providers, allows SMBs to adopt MEM and other Microsoft 365 tools without integration or deployment complexities that can challenge smaller firms.

Challenges

- Some customers IDC spoke with said that Endpoint Manager capabilities for managing non-Google Android devices (e.g., devices running the Android Open Source Project version of the

OS) are not as strong as some competitive products. Microsoft says it is planning to release enhanced support for AOSP endpoints, such as Meta's Oculus VR headsets, in 2022.

- While Microsoft's frontline/ruggedized device management approach is broad, it does not support some popular and widely used endpoint IoT operating systems and device types, such as Apple TVs, some wearables, Raspberry Pi, Samsung Tizen devices, and Linux. (Linux is on Microsoft's near-term support road map for 2022.)
- While the market for UEM technology has evolved and shifted from mobile-centric partners (carriers such as AT&T and Verizon) to enterprise software vendors and resellers, there is still a segment of the market that looks to carriers as a primary partner for deploying device management (mobile in particular). On this front, Microsoft has fewer relationships and partnerships in the wireless carrier space compared with other vendors in this market.
- MEM supports most core macOS management scenarios natively in the product, with support for macOS MDM protocol configurations. Microsoft has also partnered with Apple management specialist Jamf to enhance Apple device management with MEM (particularly around macOS management). On its own, Endpoint Manager has fewer native, deeper-level macOS support features and functions compared with other UEM solutions offering standalone macOS management features.

Consider Microsoft When

Consider Microsoft's Endpoint Manager offering for most UEM deployment scenarios, ranging from general PC and mobile device management and configuration to specialized use cases (e.g., ruggedized/frontline worker devices, workspace IoT, and temporary/seasonal contractor support).

Miradore

Miradore is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Miradore, a Finish systems management software vendor, founded in 2005, provides a range of UEM management features targeted at midsize and small companies along with a well-packaged go-to-market approach that utilizes managed SPs to host and deliver its technology.

Miradore's partnering model allows managed SPs and other service providers to easily layer the UEM technology on top of end-user computing solutions and services, such as the emerging device-as-a-service (DaaS) model, where all functions of end-user computing — from device hardware and software to infrastructure/management and security platforms — are delivered as a service. The company also focuses on SMB customers, a segment that larger EMM/UEM providers do not target with specific offerings other than stripped-down versions of larger platforms.

Strengths

- Mirador offers a SaaS-based Miradore Online UEM product and its on-premises Miradore Management Suite. This allows the company to address both cloud-focused customers and regulated industries where on-premises delivery models are preferred.
- The platform can converge endpoint management functions for smartphones, tablets, and PCs across the range of ownership models (corporate liable to BYOD, choose-your-own device, etc.).
- The suite goes beyond UEM functionality into other endpoint computing support functions, including device image/data backup services, remote control for IT support, and IT asset management. Being EU based, with a SaaS product, the company can also address data security/privacy concerns and is well ahead of GDPR compliance regulations.

Challenges

- Miradore competes more directly with larger UEM players, which are gaining presence in the EU market and serving customers there with SaaS/security requirements with reginal datacenters. The company has a relatively small footprint in terms of sales/product teams in the United States and is not as widely known in the North America EMM market (the largest market segment worldwide) compared with its larger, United States–based rivals.
- Miradore does not have many partnerships with mobile threat management software, cloud security, or identity and access management platform providers compared with competitors.
- While well established in Europe, the vendor is not as widely adopted in the United States, which is the largest regional market for UEM software.

Consider Miradore When

Consider Miradore if you are a small/midsize firm primarily based in the EU. Companies looking for SaaS-only UEM solutions should consider Miradore, as it has a strong cloud go-to-market approach, selling its software to SaaS-focused managed SPs serving the small and midmarket IT markets.

Quest Software

Quest Software is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Quest Software is a 34-year-old IT infrastructure software vendor based in Aliso Viejo, California. The vendor offers a broad range of enterprise software products ranging from UEM to identity, security, data protection and storage, IT service management, and other areas. In UEM, Quest UEM is the evolution of the company's KACE product line for PC and endpoint device management. Quest UEM combines the technology of the KACE on-premises device management appliance (or virtual appliance) with a cloud-based, modern management SaaS platform targeted at PCs and Macs, as well as mobile devices.

Custom profiles for Windows can also be supported on Windows 10/11 devices, allowing specific templated endpoint device types to be pushed down to Microsoft PCs without the need for deploying GPOs to the devices (profiles are enabled entirely via MDM protocol-based functionality).

Quest has strong Mac support functionality and supports the Apple Business Manager functions for automatic deployment, provisioning, and app distribution via corporate-owned App store software. An open REST API can be leveraged for automated management functions and workflows, such as large-scale settings controls, software package pushes, or rollbacks. Also on the automation front, Windows Autopilot, Android zero-touch, and Samsung Knox enrollment are supported for PC and mobile setups.

Strengths

- Quest has a broad product portfolio, including identity management (One Identity) database administration (Toad), data protection and backup (QoreStor, NetVault), and Microsoft environment management (GPO Admin, Enterprise Reporter). Quest UEM integrates well with each of these adjacent IT products in the Quest Software family and can provide strong TCO for organizations looking for single-vendor efficiencies.
- Quest UEM's hybrid capability for on-premises and cloud/modern endpoint management make it a strong platform for helping companies either migrate from on-premises to cloud device management or operate in a permanent hybrid state, where some devices are managed in the

cloud with modern MDM protocols, while others are addressed with traditional PCLM management functions.

- Quest UEM is among a small number of UEM solutions that can support server operating systems (Windows Server, Linux, and Unix), which makes it a strong product for managed SPs or SMBs looking for multiple device management consolidation.
- IoT endpoint is another strong point of Quest UEM with support for Linux, Raspberry Pi OS, and other IoT-centric and nontraditional endpoint device operating systems.

Challenges

- Quest has strong MDM-based Mac support features, but some UEM competitors have more comprehensive macOS control and policy enforcement capabilities around provisioning, identity binding, and integration, and support for macOS kernel access controls.
- Quest is very much a PC-centric endpoint management vendor, which also supports mobile devices. However, it has a few partnerships with carriers and is not sold through carrier channels at all. For customers looking for UEM software procured and enabled via an enterprise mobility solutions provider or channel, Quest has limited coverage.

Consider Quest Software When

Organizations with broad Windows PC footprints with emerging mobility management needs should consider Quest UEM as an UEM platform. SMBs especially (sub-1,000 worker organizations) should consider Quest for its strong functionality across multiple IT systems. Quest should also be considered by large enterprise organizations, especially in environments where multiple thousands of endpoints are supported by a small IT staff (e.g., two or fewer admins).

Samsung

Samsung is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Founded in 1938 in Seoul, South Korea, Samsung is a global maker of smartphones, consumer electronics and appliances, networking equipment, and many other product technology and product categories. The vendor's UEM product, Samsung Knox Suite, is a package of cloud-based device management services, consisting of Knox Manage, Knox E-FOTA (Enterprise Firmware-Over-The-Air), Knox Mobile Enrollment, Knox Platform for Enterprise, and Knox Asset Intelligence. Originally launched to support Samsung's Android devices, Knox Suite is now capable of managing Apple mobile devices (iPhones and iPads) as well as Windows PCs and Chromebooks. The UEM offering ties in closely with the Samsung Knox platform — a device-level security and management framework for enforcing policy and securing data on Samsung smartphones and other devices.

Knox features on Samsung devices — which integrate strong encryption, OS and app protection, and hardware integrity — can be easily enabled and configured via the Knox Manage. In addition, Knox Manage provides monitoring, management, and control of policy on Apple devices as well as endpoint configuration for Windows and Chrome OS. Device provisioning services such as Apple Business Manager, Knox Mobile Enrollment, and Android Enterprise Zero-Touch Enrollment are supported by Knox Manage as well.

Knox Manage also lets IT administrators efficiently manage the devices of frontline workers by remotely accessing employee devices to troubleshoot, tracking device locations, and dynamically applying policies based on user environment (such as unlocking the camera function when the user heads out from the

office). Knox Manage is Android Enterprise recommended and supports three advanced feature sets including the Android Enterprise Dedicated Device profile, as defined by Google.

Particular to Samsung devices, Knox E-FOTA can be used to deploy a particular OS version that IT admin has fully tested across device fleet without user interaction. Using Knox Asset Intelligence, device usage insights, such as battery/app usage trend and connectivity issues, can be easily checked by IT admins to optimize the employee workflows.

Strengths

- Knox Manage is optimized for Samsung Android device support, including comprehensive device management features (including usage and use case customizations of hardware such as physical button functionality). This is especially useful for frontline worker device deployments.
- Device management, OS version control, remote troubleshooting, and asset intelligence features of Knox Suite are a strength for supporting ruggedized devices or endpoints that spend their entire lifetime in the field, without coming into a central office or IT shop for upgrades or maintenance.
- FIPS 140-2, SOC2 and NIAP CC certified, Knox Suite is redundant across three major regions (North America, Western Europe, and APAC [Singapore/India]).
- Samsung has deep console integration capabilities with several mobile threat management vendors for integrating on-device threat detection on mobile devices with the UEM product (Check Point, Pradeo).
- Chromebooks (Samsung or other OEM's) can be managed via Knox Manage, with the ability to manage device-level settings and configurations.

Challenges

- Samsung Knox Manage does not support macOS.
- Knox Manage supports a growing number of Windows device management via managed SPs, but it does not support deeper levels of Windows management, such as GPOs or script-based policy enforcement or controls.
- Knox Manage does not support Windows Autopilot for automated device provisioning (will be supported in August 2022).

Consider Samsung When

Businesses should look to Samsung Knox Suite if they are using Samsung devices extensively in their environment, including smartphones, tablets, and Windows PCs (Samsung manufactures Windows-based laptops). Organizations with specific use case requirements for mobile device in the field — ruggedized endpoints, remote troubleshooting, location tracking, and single-purpose deployments — should consider Knox Suite, either as a primary or as an additional UEM product in their overall IT infrastructure environment.

Sophos

Sophos is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Founded in 1985, the United Kingdom-based Sophos is a 4,000-person cybersecurity software and hardware vendor focused on SMB and midsize enterprises, with products spanning endpoint security,

network security, security analytics, and endpoint device management. The company's UEM product, Sophos UEM, is an evolution of Sophos Mobile MDM/EMM platform. The product now supports four major operating systems (Windows, macOS, iOS, and Android), with some support for Chrome OS, and integrates tightly with the company's security technologies.

The company's Sophos Central console is a centralized management and monitoring platform spanning all its security tools, as well as the Sophos UEM product. Sophos XDR (extended detection and response) is another tool tying into UEM. The XDR product includes a data lake and data analytics tool, which now allows customers to store and access device state and security compliance information across all UEM-managed devices. The platform allows for offline management and scanning of endpoint device states/network logs; iOS and Android devices can now upload data into the XDR data lake.

The UEM product can also be pulled into automated response actions, as orchestrated by Sophos' Refactr technology (a response automation vendor the company acquired in 2021). This could allow UEM to be utilized as an enforcement point to remediate detected breaches, suspicious activity, or detected malware on devices. (This might include shutting down a PC or mobile device's network access to corporate resources, shutting down specific apps or processes running on the device, or other remediation tasks.) Having UEM and device state data in the data lake also allows customers to trend usage patterns and device state over time and apply security policies based on trending activities and use cases.

Sophos supports the Apple Business Manager device management enrollment as well as Android Enterprise (Work, Device, Dedicated, and OEMConfig profiles) and Samsung Knox Platform for Enterprise (KPE). Devices such as Chromebooks can be managed via Chrome Extension security policy management and MAM-based controls on Android apps deployed on Android. Users can also onboard Windows 10 devices with Windows Autopilot automated setup and configuration service and enroll into Sophos UEM. While Sophos emphasizes its centralized dashboard and management tool, the company can deliver this centralized experience in multiple scenarios, including traditional admins, as well as a version for partners and managed service providers that host/resell Sophos UEM and security products for customers.

Strengths

- Sophos has extensive resale partnerships with more than a dozen mobile/cellular carriers — key partners in terms of reaching enterprise and SMB mobility customers — including three of the four major U.S. carriers, as well as major operators in Europe, Asia, and Latin America.
- Sophos Intercept X for Mobile, an MTM application, is a strong on-device threat detection solution for Android and iOS devices, which is the primary focus in terms of mobile security software deployments for smartphones. This product is tightly integrated into Sophos Mobile and UEM solutions, as well as the larger Sophos Central security management architecture.
- Sophos' web and antiphishing; capabilities extend to its UEM platform, allowing browser-based mobile and PC activity to be monitored and acted upon (in the event of breaches or security events) from a single UEM console.
- With a core focus on the SMBs and midmarket enterprises, Sophos' broad portfolio of cybersecurity, networking, and analytics products offers customers a broad range of integration opportunities with its UEM product, strengthening the management offering as part of a larger Sophos security/management platform. It's particularly focused at small and single-

person IT/security teams, as well as managed SPs, that have to manage large numbers of devices with a small group and resources.

- Sophos supports IoT device management scenarios such as conference room digital media management (Apple TVs [tvOS] and Watch [watchOS]); Android Things, Raspberry Pi, and the Tizen IoT operating system are also covered. Sophos NAC can also figure into IoT endpoint use cases in conjunction with Sophos UEM.

Challenges

- While customers with the entire Sophos security stack get value out of UEM integration across Sophos products, Sophos UEM is not seen as much as a standalone UEM solution on its own, especially for large enterprise deployments with complex Windows device management policies and strict mobile device usage control requirements.
- While Sophos has strong server endpoint security and monitoring capabilities, it does not have direct device management, configuration, and monitoring tools tied to its UEM product. Other vendors, with a focus on SMB and converging multiple security and management tools into a single platform, are further along than Sophos on this front.

Consider Sophos When

Large organizations should consider Sophos UEM if they already use Sophos security products (endpoint, network, content security, etc.) and want to tightly integrate endpoint device management with security. SMBs should look at Sophos UEM as well as a way to consolidate multiple products with a single vendor while having tight integration among point products.

SOTI

SOTI is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

SOTI is among the few standalone EMM/UEM vendors in the market overall, with a focus on the management of ruggedized mobile devices. SOTI has wide adoption for EMM of computing endpoints deployed in environments such as warehouses, factories, and airports, as well as in field services, retail, and medical scenarios. The SOTI MobiControl product is the main UEM offering providing MDM, MAM, and MCM capabilities from a single code base via on-premises or cloud-delivered software. While some SOTI customers interviewed for this study used MobiControl for all mobility use cases, several others said they used MobiControl to manage legacy and modern ruggedized devices, as well as other user-interfacing IoT-like endpoints, alongside another third-party EMM solution for other mobility use cases.

Strengths

- While known for ruggedized and IoT mobile endpoint management, SOTI has supported macOS since 2018. It has extended this capability to include support for deploying apps, enforcing configuration settings (e.g., Wi-Fi and VPN settings), and enrolling in device inventory and monitoring functions via SOTI's UEM platform.
- SOTI's greatest strength is the breadth of device types it supports — from legacy Windows CE, NT, and XP platforms to Linux devices, bar scanners, mobile printers, and other ruggedized single-purpose devices and smartphones. This has led to many customers using SOTI specifically for management of these types of devices, even with the presence of another EMM platform.

- SOTI's MADP and mobile help desk capabilities are unique. SOTI does not have to partner with other specialist vendors, or integrate products from separate business units, to approach such an offering.

Challenges

- While well-recognized in ruggedized and field service mobile technology deployments, SOTI is not as widely known for supporting traditional mobile knowledge workers, which is a much larger addressable market in terms of growth and potential seat expansion.
- SOTI has outlined larger ambitions in product road map briefings around larger IoT initiatives, mobile application development, and rapid app dev solutions as well as worker productivity apps, but it has not fully delivered on these initiatives or articulated a larger strategy for the company.
- SOTI has limited partnerships and support with other third-party identity and cloud application security broker technologies, limiting the ability to support cloud-based SSO or integrations with other identity platforms.

Consider SOTI When

Consider SOTI when your organization requires management, security, and policy control over a wide range of ruggedized mobile devices, legacy OS devices, or specialty handheld devices and peripherals. Small to midsize enterprises with ruggedized devices may consider SOTI for all UEM device deployments. Larger enterprises with ruggedized/IoT needs may consider SOTI as a separate solution for those specific use cases.

VMware

VMware is positioned in the Major Players category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Founded in 1998 in Palo Alto, California, VMware is a large enterprise system infrastructure software vendor, with roots in server and desktop virtualization. Its UEM product, VMware Workspace ONE, has evolved from technology acquired when it bought EMM/MDM vendor AirWatch in 2014. Workspace ONE has since become more deeply integrated with the vendor's desktop virtualization, security, networking, and identity and analytics technologies.

Workspace ONE addresses a broad range of device types and use cases across vertical industries, from traditional mobility management to modern Windows PC and Mac management and IoT device management. The UEM component of Workspace ONE is also part of a broader product portfolio from VMware's end-user computing group, including VMware Horizon desktop virtualization, endpoint and application analytics, and endpoint security based on technology acquired in the purchase of Carbon Black.

VMware made a number of improvements and advancements in Workspace ONE in 2021, including augmented management capabilities for Apple's macOS devices, as well as Windows management. Apple device enrollment has also been expanded in Workspace ONE, such as provisioning and enablement of native Mac and SaaS-based apps for productivity. The provisioning also extends to device-level user/admin accounts and allows for Macs to be directly configured for corporate identities out of the box. On the Windows front, Workspace ONE now includes Drop Ship Provisioning of corporate Windows PCs from Dell, as well as Lenovo and HP Inc. The Drop Ship Provisioning Online function allows for a Windows Autopilot-like provisioning experience without the need for Azure AD Premium purchase, which sets up devices pre-shipment in the OEM or partner factory imaging

process, including deeper levels of configuration such as Group Policies, Win32 apps, identity and Active Directory domain registration, and setup.

VMware also integrates with ITSM vendor ServiceNow to allow administrators to launch end-user support functions such as remote device locking, remote takeover, and screen viewing right from the ServiceNow interface, without having to change to a Workspace ONE console.

Strengths

- Digital Employee Experience Management is an evolution of VMware Workspace ONE Intelligence. The Digital Experience technologies can measure device-level and app-level performance of technology, such as devices with poor battery health, slow boot-up, or crashing apps, and network performance, and calculate experience scores based on all these inputs and monitored metrics.
- Workspace ONE Freestyle Orchestrator tool, intended for IT teams to create automated management orchestration workflows, also saw traction among Workspace ONE customers with UEM customers deploying this technology in their environments. Workspace ONE also includes end-user-focused automation tools, such as Workspace ONE Experience Workflows for quick task and end-user workflow integrations within the Intelligent Hub user interface.
- Workspace ONE Assist is another add-on function that expands the scope of the company's UEM product further – in this case, to remote device management and screen viewing. This allows IT teams to view or take over the main screen or user interface of a supported Windows/Mac/Linux device, virtual desktop, as well as iOS/Android devices – a key criterion for supporting frontline/ruggedized endpoint management use cases.
- VMware has also extended app-based VPN tunneling to nonmanaged endpoints (via VMware SD-WAN function) as part of the company's larger VMware Anywhere Workspace technology, which incorporates UEM and SD-WAN technologies.

Challenges

- While VMware has done a good job packaging its adjacent products around Workspace ONE (e.g., Anywhere Workspace, combining UEM, endpoint security, and SD-WAN), some customers still see the functional integration among products as lacking. In particular, integrations of the acquired Carbon Black endpoint security software with Workspace ONE are still limited and operate as if the products are offered by two separate companies, users said.
- Some customers IDC spoke with for this study said that data extraction and reporting in Workspace ONE was difficult to set up. Data accuracy and consistency of reporting were also areas where Workspace ONE users said the product needs improvement.

Consider VMware When

Consider VMware for all UEM deployment scenarios, especially where management software platform consolidation and reduction is a core requirement, as Workspace ONE is capable of handling nearly all endpoint management scenarios as a standalone system.

Zoho (ManageEngine)

Zoho (ManageEngine) is positioned in the Leaders category in this 2022 IDC MarketScape for worldwide UEM software for SMBs.

Zoho, founded in 1996 and with worldwide headquarters in Chennai, India (and U.S. headquarters in Austin, Texas), is a maker of business SaaS products for enterprises and SMBs. The vendor has a

worldwide reach and sells its CRM, ERP, productivity, and IT infrastructure software across all global markets. The vendor's UEM product, ManageEngine Endpoint Central, is part of the larger ManageEngine business unit that covers IT infrastructure and security software products.

ManageEngine Endpoint Central supports the five major endpoint operating systems (Windows, Mac, iOS/iPadOS, Android, and Chrome) as well as legacy Windows and Linux. The product also supports ruggedized and IoT endpoint OSs such as Zebra, Honeywell, and Datalogic devices as well as Apple tvOS, Microsoft HoloLens, and Google Glass. Wearables (Google Glass and Microsoft HoloLens), ruggedized devices (Zebra, Honeywell, and Datalogic), and IoT endpoints (Apple TVs) are also supported. While most Zoho products are SaaS/cloud, ManageEngine Endpoint Central can be deployed either as on premises or via SaaS and can support both off-network and on-network management use cases.

ManageEngine develops and markets system infrastructure software products targeted at SMBs and enterprises. Its UEM product ManageEngine Endpoint Central is an evolution of its separate Desktop Central and Mobile Device Management products. It has a broad portfolio of IT tools, including ITSM (ManageEngine Service Desk), endpoint security, analytics tools (ManageEngine Analytics Plus), and IT asset management (ManageEngine Asset Explorer), as well as tools for managing Active Directory deployments. These offerings integrate tightly with ManageEngine Endpoint Central and can provide SMBs with a strong single-vendor approach to most end-user computing management and security functions. There is also an endpoint security add-on capability to ManageEngine Endpoint Central, which combines antimalware with endpoint management in a single package.

Strengths

- Patch management is one of the main capabilities across Windows and Mac platforms (as well as Linux) as well as extensive patch and vulnerability management support for third-party apps and software on both platforms. It also supports broader automation of PCLM routines such as patches, deploying software and OS imaging (in addition to mobile device management and application management).
- ManageEngine Endpoint Central is among the most price-competitive UEM products evaluated in this study. The vendor also has competitive bundling and add-in pricing discounts for products across its portfolio, which could be attractive to price-sensitive enterprises or SMBs looking for broad high-function/low-cost endpoint management solutions.
- ManageEngine Endpoint Central includes remote help, screen view, and remote management/takeover of endpoints, allowing IT help desk teams to walk through and show or remotely execute administrative tasks and functions.

Challenges

- While Zoho/ManageEngine offers a large portfolio of apps and platforms for enterprise IT beyond UEM, it does not integrate widely with third-party security products and technologies such as security information and event management, endpoint security, and mobile threat management. However, the vendor is in the process of expanding partnerships with threat intelligence vendors and recently partnered with CrowdStrike. It also supports the three major cloud identity platforms: Microsoft, Okta, and Ping.
- The Zoho and ManageEngine brands, while widely deployed and known in the SMB market, do not have as much awareness in the enterprise space. Among enterprise IT decision makers (at firms with more than 1,000 employees) IDC interviewed for this study, few had ManageEngine on their short list of potential UEM providers. To address this, Zoho

(ManageEngine) plans to go to market with strategic systems integrator partnerships (Accenture, IBM, NTT Global and Lockheed Martin) with plans to specifically target the enterprise sector.

Consider Zoho (ManageEngine) When

Consider Zoho (ManageEngine) when your organization is already standardized on ManageEngine from a service desk and/or PCLM platform perspective. Adding the UEM capabilities to an existing ManageEngine environment can be a quick and efficient way to introduce UEM practices into a business, especially for the midsize and SMB customers using ManageEngine that may not have budget or capability to adopt and absorb a larger, more complex and costly UEM solution.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Unified endpoint management (UEM) is a technology submarket category of the client endpoint management functional software market. UEM solutions combine into a single software platform the management and provisioning functions for most common end-user computing operating systems (i.e., Windows, macOS, iOS, Android, and Chrome OS) and device types. By definition, UEM products must be able to manage both mobile and PC endpoints; this excludes legacy platforms such as PC life-cycle management (PCLM), PC imaging solutions, and mobile device management (MDM).

Strategies and Capabilities Criteria

Tables 1 and 2 provide market-specific weighting definitions and weighting values.

TABLE 1

Key Strategy Measures for Success: Worldwide Unified Endpoint Management Software

Strategies Criteria	Definition	Weight (%)
Delivery	▪ The vendor has the delivery model for the product and associated support and maintenance services for future customer needs.	12.0
Financial/funding	▪ The company will generate, attract, and manage capital well over the next three to five years to create market value.	3.0
Functionality or offering strategy	▪ The vendor's current development of offerings will be relevant and attractive to customers over the next three to five years.	3.0
Growth	▪ Over the next three to five years, the vendor's sales/distribution structure will be aligned with the way customers, especially those in high-growth market segments, want to buy. ▪ Partner/channel strategy is expected to extend over the next 12–18 months.	47.0
Portfolio benefits	▪ The vendor has a strong portfolio of adjacent and complementary products and services relative to the main product being analyzed in this study.	31.0
R&D pace/productivity	▪ The pace of continued investment is expanding the company's industry cloud offerings over the next three to five years.	4.0
Total		100.0

Source: IDC, 2022

TABLE 2

Key Capability Measures for Success: Worldwide Unified Endpoint Management Software

Capabilities Criteria	Definition	Weight (%)
Customer service delivery/satisfaction	▪ The vendor's customer-facing delivery capabilities satisfy market wants and create a strong level of value for its customers.	13.0
Growth	▪ The vendor's installed base of users will help it grow the sales of adjacent and complementary products	1.0
Functionality or offering	▪ The vendor's capabilities maximize the connection between offerings and customers, such as delivery, partnerships, pricing, distribution, marketing, sales, and service. ▪ Reporting capabilities and other features are available across on-premises and cloud-delivered offerings.	62.0
Portfolio benefits	▪ The vendor has a strong portfolio of adjacent and complementary products and services relative to the main product being analyzed in this study.	20.0
Pricing model or structure of product/offering	▪ The vendor is willing to demonstrate value through flexible pricing mechanisms, including profit sharing–based relationships.	3.0
Total cost of ownership (TCO)	▪ The product provides customers with strong TCO capabilities due to inclusiveness of features and functions, reduction/savings in operational/acquisition costs, and overall value.	1.0
Total		100.0

Source: IDC, 2022

LEARN MORE

Related Research

- *IDC Market Glance: Client Endpoint Management, 1Q22* (IDC #US48969122, March 2022)
- *Top 5 Trends in Unified Endpoint Management to Watch in 2022* (IDC #US48779022, February 2022)
- *Top Technology Integration Opportunities for Unified Endpoint Management* (IDC #US48266821, September 2021)

Synopsis

This IDC study represents a vendor assessment of providers offering unified endpoint management (UEM) software through the IDC MarketScape model, with a focus on the SMB market. The assessment reviews both quantitative and qualitative characteristics that define current market

demands and expected buyer needs for UEM software. The evaluation is based on a comprehensive and rigorous framework that assesses each vendor relative to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the UEM market over the short term and the long term.

"SMBs across all industries are adopting sophisticated endpoint device use cases and deployment models, targeting the same level of efficiency and productivity as larger firms," says Phil Hochmuth, program vice president, Endpoint Management and Enterprise Mobility at IDC. "At the same time, SMBs look for greater levels of integration, automation, and product portfolio from the UEM technology suppliers. Vendors targeting this market must take into account these additional needs."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com