IDC MarketScape

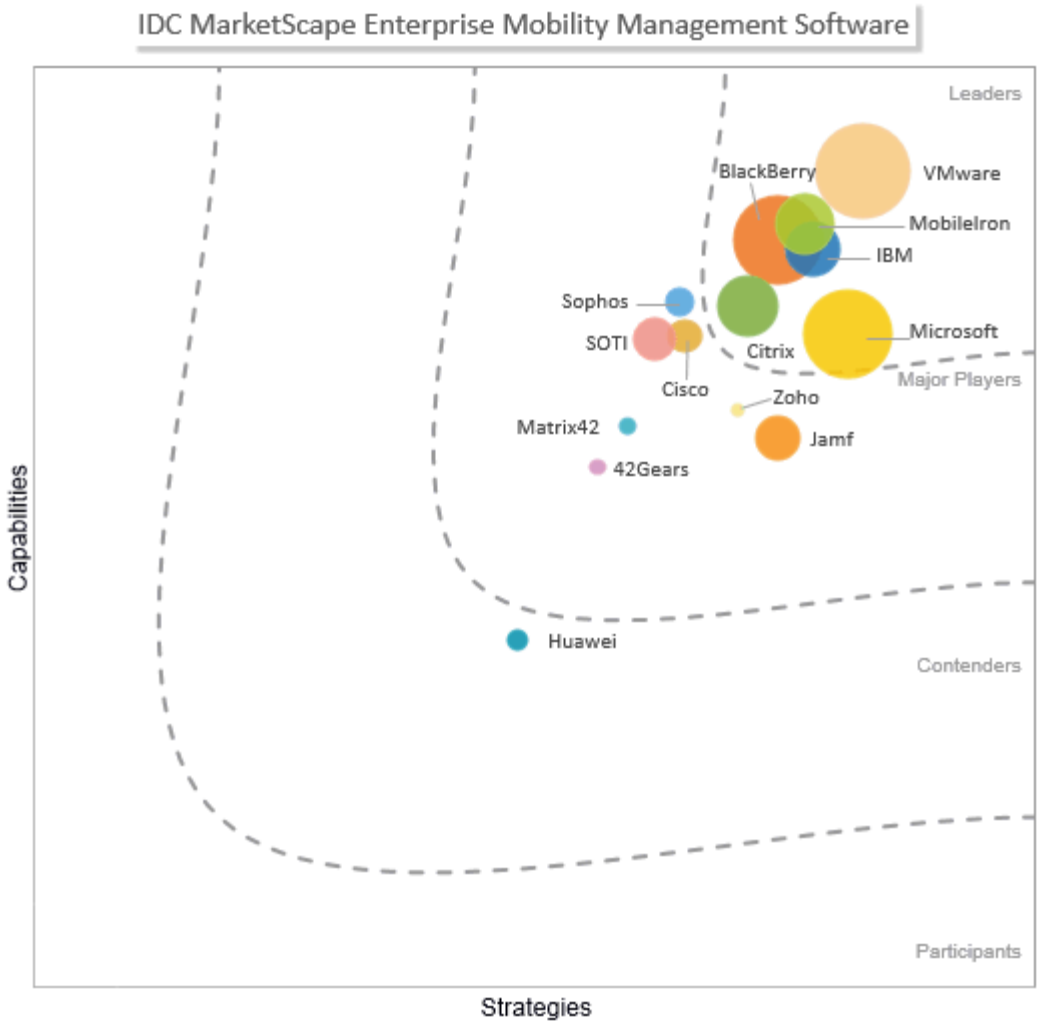
IDC MarketScape: Worldwide Enterprise Mobility Management Software 2018 Vendor Assessment

Phil Hochmuth

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Enterprise Mobility Management Software Vendor Assessment



Source: IDC, 2018

July 2018, IDC #US43294018

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

IDC OPINION

The enterprise mobility management (EMM) has moved from a specialized mobile device-centric configuration platform to a broader role, managing, securing, and enforcing policy on a wide range of endpoints, from mobile devices to PCs and smart connected enterprise IoT endpoints. Strong adoption of the technology among U.S. enterprises (more than 80% say they have some EMM platform deployed, according to IDC's 2018 *Enterprise Mobility Software Decision Maker Survey*) is reflected in double-digit growth in market revenue over the past several years. Unified endpoint management (UEM) is a single software platform that controls both PC and mobile endpoints. According to IDC's survey, over 40% of enterprises deploy EMM for some PC management, and more than a third are using EMM in IoT-centric use cases

This study is the first in a series of three IDC MarketScapes that considers all major use cases and broad functionality requirements for EMM solution providers in the market, including PC management and UEM use cases as well as IoT use cases. Subsequent IDC MarketScapes will provide specific analysis of vendors' EMM software capabilities and strategies with regard to PC and UEM management deployments and IoT/ruggedized device use cases. This EMM market evaluation took into account current capabilities of EMM products relative to mobile and PC devices and a vendor's strategic plans around future IoT expansion. Vendors with leading offerings in the EMM market provide this breadth of capabilities today with product development road maps that will match future needs. Key findings include:

- EMM vendors generally meet most requirements of today's enterprise mobile device and application management functions across the most relevant mobile operating systems (Apple iOS and Google Android).
- UEM capabilities in EMM platforms are mainly focused on Windows 10 management, although legacy Windows PC OS support is available by some EMM vendors. Mac OS management is growing, as well as Google's Chrome OS.
- IT buyers looking at EMM software today are looking closely at solutions with future UEM and IoT capabilities in mind.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Because of the large number of vendors participating in the EMM market, IDC invited vendors to participate based on two key criteria:

- An EMM suite offering mobile device management (MDM), mobile application management (MAM), and mobile content management (MCM) capabilities
- EMM product revenue of $10 million or above for calendar year 2017 (Revenue was estimated in April 2018 and may differ from forthcoming vendor share documents.)

In addition to the companies profiled in this study, there are also a number of other companies in the EMM market with relative products that did not meet the vendor inclusion criteria for this study. These include Amtel, baramundi software, CA Technologies, Kaspersky Lab, Kony, Miradore, Prey Software, and Snow Software.

ADVICE FOR TECHNOLOGY BUYERS

This study analyzed and rated vendors across a broad range of capability- and strategy-focused criteria. Technology buyers should evaluate EMM platforms with feet in the present (mobile device/app management and security) and clear eyes on the near future of UEM and enterprise IoT device management requirements. To that end, the criteria and attributes that are key for IT buyers to consider when evaluating EMM platforms are discussed in the section that follows.

Key Measures for Success

- **Core functionality of EMM platforms in the areas of MDM, MAM, and MCM.** Core functional components also include secure PIM, DLP and file access controls restrictions, app wrapping, and SDK capabilities. While EMM platforms are evolving to new use cases and management tasks, these core EMM platform capabilities are still a baseline requirement.
- **Strong portfolio of adjacent and complementary IT products, services, and solutions.** Solutions such as endpoint security, identity, VPN, network access control (NAC), mobile devices, mobile applications or app development platforms, virtualization, and data/analytics capabilities all have relevant tie-ins with EMM platforms.
- **Ability to support a broad range of device operating systems.** iOS and Android are the dominant two mobile operating system (OS) platforms in the world, but others do exist, and new ones are emerging in certain regions and industries. Also the extension of EMM platforms into PC and IoT management scenarios requires support for new types of devices and OS software, from PC operating systems to wearables and other embedded real-time OS technology in IoT endpoints.
- **Adjacent mobile security integration.** With the increased focus on mobile security and the endpoint, EMM vendors that support integration with a broad set of mobile threat management (MTM) and other relevant security technologies (identity platforms, threat analysis, etc.) will be better positioned against vendors with limited partnerships or integration capabilities.
- **Intelligence and analytics.** With such a broad view of endpoint and end-user activity, EMM 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. EMM vendors with strong analytics and reporting capabilities around these key metrics will have competitive advantages over vendors not focusing on this area.
- **Capabilities for supporting noncorporate devices or BYOD users.** Support for employees personal mobile, or BYOD, is critical to expanding seats and overall management scope of an EMM platform. With over 90% of enterprises supporting BYOD, businesses must find tools that can apply to these devices the same levels of granular policy enforcement, security and control over apps, and data accessed by these devices as corporate-owned device.
- **Conditional access controls and policy enforcement triggers.** This is becoming a critical feature of EMM platforms. Conditional access controls what apps, data, or other resources a user can connect to and consume, based on array of factor, 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 jailbroken/rooted device or an OS that is out of date).
- **Scalability and cloud-based delivery capabilities.** Cloud is the future of the EMM market as most vendors offer some level of this delivery model. SaaS-based EMM fits with the mobile/cloud synergies of enterprise mobile computing, allowing businesses to flexibly deploy EMM capabilities to mobile devices wherever they are, without having to stand up and

maintain on-premise servers and supporting IT resources. Hybrid is still an important aspect of EMM as many organizations still require some on-premise deployment scenarios, particularly security-sensitive industries such as financial and government, or in deployments in EU countries with more stringent cloud data privacy regulations.

- **Strong UEM capabilities and road map for customer success.** While EMM platforms today mostly manage smartphones and tablets, laptop and PC management (both Windows and Mac) as well as emerging Google Chrome OS devices are increasingly being considered for management with EMM. Unified endpoint management is on the road map for the majority of U.S. enterprises, but this will not be an easy cutover; organizations will need help transitioning from PC life-cycle management (PCLM) platforms to UEM-based solutions. Critical support issues will involve transitioning Win32, PC image management, patching and update packages, and group policy objects to EMM-based modern management.
- **A pragmatic and scenario-driven IoT strategy for EMM.** EMM platforms are not the answer for all IoT scenarios. Businesses will not likely want to manage IoT-connected oil wells, shipping containers, livestock, or other industrial IoT activities with the same platform as mobile phones and laptops. However, it is logical to extend EMM management functionality to enterprise-focused IoT scenarios that integrate connected office technologies (physical access), connected conference rooms, user/asset location tracking, data entry/transactional kiosks, and wearables. Enterprises will look to a UEM platform provider to support these deployments.

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 a Major Player in the 2018 IDC MarketScape for EMM software. 42Gears, based in Bangalore, India, with operations worldwide, has been in the device management business for nine years. The company provides a wide range of products, from basic MDM solutions in its SureLock product to a full-featured UEM solution in SureMDM. The company has found success in locked-down device management deployments that require consistent, easily configurable kiosk or single-app features. However, 42Gears goes beyond this use case, with support for secure email, PIM, app wrapping, and all major EMM features. 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.

Strengths

42Gears has a strong remote management capability, allowing IT administrators to view an end user's device 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 polices.

42Gears UEM uses native platform DLP frameworks, like Android Enterprise and iOS MDM protocol, to segregate personal and work app data (including MS 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, from PCs (Windows 7 and 10 and Mac OS) to Android, iOS, Linux, Raspberry Pi, and Unix-based devices. This allows the software to address a wide range of mobility, UEM, and IoT use cases.

Challenges

42Gears has limited support for Office 365 application policy enforcement, containerization, or data security features for mobile Microsoft apps.

42Gears has limited support or integration with third-party MTM software, identity platforms, or cloud access security broker (CASB) solutions, limiting the enablement of more advanced mobile security and access control scenarios.

42Gears is not widely recognized as a platform for managing PCs, as it has traditionally focused on the EMM/MDM markets. It's UEM solution is relatively new (introduced in 4Q17) and has not gained as much market traction or recognition as competitors with products in the market longer.

Consider 42Gears When

Consider 42Gears for deployments where endpoint lock-down, single-app use, and other IoT-focused device management features are required. 42Gears is not limited to just this scenario, but it is a strong point for the company's products. For organizations looking to manage every endpoint scenario from a single platform (EMM, UEM, and IoT), 42Gears should be considered, especially for midsize and small enterprises looking to consolidate management platforms and create unified management policies.

BlackBerry

BlackBerry is a Leader in the 2018 IDC MarketScape for EMM software. BlackBerry's EMM portfolio includes a well-integrated suite of mobile device, application and content management, and enablement capabilities, combined with strong security features and an overall well-integrated solution. BlackBerry's main EMM product, BlackBerry Unified Endpoint Manager (BlackBerry UEM), provides strong device management configuration and security capabilities, a long-standing strength of BlackBerry from its days as one of the original enterprise-scale MDM platforms. BlackBerry had strong MAM capabilities prior to its acquisition of Good Technology, but the inclusion of the Good Work Suite, now BlackBerry Work, as well as its strong app-level policy controls and security settings make this one of the stronger MAM solutions on the market. From a mobile content management standpoint, BlackBerry Workspaces (formerly WatchDox) file sync and share technology is a strong cloud-centric content management system, with specific features around security, data confidentiality, and rights management.

Strengths

BlackBerry has made strides in unifying its console and user experience for managing multiple device types, such as wearables, multi-OS PC support, and other connected endpoints.

The company's NOC infrastructure provides strong cloud-based connectivity to internal apps and assets without requiring extensive firewall or VPN port enablement. Connection to this network, basically a combined cloud-based remote access, threat detection, and connection brokering platform, strengthens the overall EMM offering.

BlackBerry Access is a secure browser solution which augments the company's UEM strategy, providing access to behind the firewall intranet applications access, as well as cloud application

access controls and policy enforcement. BlackBerry positions this as an alternative to heavier-duty desktop/app virtualization models from some use cases.

BlackBerry's Radar platform, an IoT for management and tracking service, as well as the company's QNX real-time IoT operating system, provide BlackBerry strong technology background and credibility in the emerging IoT space.

Challenges

BlackBerry's strength in security and compliance for mobile devices is seen as somewhat overkill for some enterprises in nonregulated deployment scenarios IDC spoke with that considered the products. BlackBerry has analytics and analysis/reporting technologies on its road map, but these are not GA today.

BlackBerry does not have an extensive portfolio of tools or features for transitioning customers from legacy PCLM tools to modern management or co-management scenarios.

Cisco

Cisco is a Major Player in the 2018 IDC MarketScape for EMM software. Cisco Meraki System Manager is a completely cloud-delivered EMM solution providing mobile device management, enterprise app store, and some mobile DLP and telecom expense management capabilities. It has strong Windows and Mac and Google Chromebook endpoint management features as well. Meraki Systems Manager is particularly strong at combining the management of a wide range of device types and device ownership scenarios, from corporate-owned and BYOD iOS, Android, Windows, and OSX devices, as well as integration of larger management infrastructure via Meraki network management capabilities overall.

Strengths

Integration and unified management of Systems Manager with Cisco products such Cisco Identity Services Engine, Cisco AnyConnect VPN Client, as well as Cisco ASA and Aironet firewall and wireless infrastructure are strong integration capabilities that will appeal to organizations managing overall mobility from a network-centric point of view.

With Cisco's partnership with Apple, Systems Manager can quickly configure and provide QoS priority to certain traffic types on iOS devices connecting to a Cisco/Meraki-based WLAN infrastructure. Simple integration with Cisco's Umbrella DNS-based web security platform is another advantage of the EMM product as well.

Cisco has one of the stronger unified endpoint management offerings in terms of unified console and code base, with the ability to apply settings which affect wide ranges of devices from a single interface. It's device/user management approach is simple, efficient, and effective.

For its combined feature set and breath of integration points, the Cisco offering was competitively priced compared with more widely deployed or known EMM platforms and market.

Challenges

Cisco Meraki Systems Manager lacks advanced app wrapping, secure PIM, and secure-managed mobile browser technology – basic offerings of many other EMM solutions. (Cisco says its approach is to provide native-based OS controls based on the AppConfig standards.)

Cisco overall has limited support and integration with third-party mobile threat management technologies, and cloud security platforms, which are increasingly key integration points for EMM platforms.

Consider Cisco When

Consider Cisco when your organization's network infrastructure is heavily based on Cisco cloud-managed WLAN, LAN, and security infrastructure, and/or Cisco's Identity Services Engine platform is used to manage endpoint network access control.

Citrix

Citrix is a Leader in the 2018 IDC MarketScape for EMM software. Citrix is a well-established end-user computing management software provider, with products ranging from app and desktop virtualization to app delivery and datacenter infrastructure software. The vendor's XenMobile product is marketed and sold as part of the company's larger Citrix Workspace offering, which is Citrix's solution for secure mobile, application, and desktop virtualization delivery. Citrix Workspace combines all elements of end-user computing management into a single platform for application and data delivery to any device type. Citrix also partners closely with Microsoft around EMM go to market and technology integration has largely been a success. Recently, Citrix rebranded XenMobile to Citrix Endpoint Management and announced the availability of a new Citrix Cloud service offering Citrix Endpoint Management. Citrix Endpoint Management will include Citrix Workspace Environment Manager which provides legacy Windows 7 and Windows 10 user group policy (GPOs) management and resource optimization.

Strengths

Citrix's recently introduced Workspace app is a well-designed single point of access tool for all Workspace services, from app access (across any device type) to provisioning new devices, as well as security functionality and cloud resource access. Citrix Workspace app also allows users to access their files using Citrix ShareFile.

Citrix is among the most forward-thinking EMM providers in terms of workspace IoT concepts and strategy. The company's Workspace Hub can create a wide range of connected enterprise and workspace IoT scenarios, such as location/presence-aware device log in, conference room meeting integration of multiple endpoint devices, as well as wearable and smart/connected peripheral integration.

The NetScaler is a competitive advantage for Citrix in terms of remote mobile worker support and scalability. The gateway's capabilities around strong remote access control, VPN, and granular inspection and security of mobile traffic help make Citrix's total EMM offering among the most advanced (from a remote access aspect) relative to competitors.

Citrix also provides a suite of secure mobile applications including Secure Mail, Secure Web, and Citrix ShareFile. In addition, Citrix provides MAM flexibility supporting native MAM, Intune MAM, and Citrix MDX technology.

Challenges

The Citrix UEM approach is focused on supporting and provisioning Windows 10, and other modern PC OSs, to modern management frameworks. Citrix Workspace Environment Manager (included with Citrix Endpoint Manager) does offer workspace management for virtual and physical Windows 7 and Windows 10 PCs for profile management, resource optimization, and user experience. However,

competitors with more capabilities could get ahead of Citrix in customer UEM trials, as many customers will move gradually to UEM, requiring migration support for Windows 7 and other related policy and app delivery frameworks, instead of a fast move to modern management. The XenMobile product has fewer telecom expense management capabilities compared with other vendors in the Leader category of the study. This capability is considered an important feature according to many enterprise telecom/IT teams responsible for mobile device management.

Huawei

Huawei is a Contender in the 2018 IDC MarketScape for EMM software. This Chinese telecom equipment and handset giant has a vast array of technology capabilities, which extended enterprise software and management. AnyOffice, a product managed under Huawei's larger enterprise network security and infrastructure group, provides mobile device management and mobile application management capabilities along with some IoT management functionality for enterprise-connected endpoints. The on-premise–only solution includes gateways for remote access VPN based on Huawei VPN appliance technology. The solution offers an integrated single management console for managing iOS in Android devices, as well as third-party connected network devices such as IP security cameras.

For large deployments of Huawei technology, from the network down to the Android handset (the third most shipped Android handset in the world), Huawei has a strong security capability. Proprietary hardware on Huawei handsets can be leveraged by the AnyOffice solution to provide advanced quick integration, as well as onboarding for Huawei Android devices. It's interesting to note that, while many EMM vendors tout their Global 1000 account references, the number 1 and number 2 companies on the Global 1000 (both Chinese banks, not by coincidence) use the Huawei AnyOffice EMM solution to manage hundreds of thousands of devices.

Strengths

Huawei has a strong on-premise solution for MDM and MAM capabilities, with the ability to extend MCM to endpoints via network-based file shares and content control and rights management capabilities.

Huawei has a unique security integration story for and deployments of enterprise mobility based on Wally technology. It is the only handset maker with EMM product on the market, and thus, it has some advantages from a standpoint particularly around hardware-based security built into Android devices. It's technology in the network security IoT gateway space is also strong points for enterprises with broader integration ambitions for EMM platforms.

Challenges

Huawei technology in general is not used widely in West among Western businesses, particularly in the United States-based organizations. While strong in markets such as the media and AIPAC, these markets are weaker in terms of EMM adoption overall, which is the challenge for Huawei in general to spread this technology user base.

The lack of cloud-based solution will be a turnoff to many enterprises considering Huawei, which only offers appliance-based capabilities for MDM and MAM. The lack of true cloud-based MCM solution, or even strong integrations with third-party cloud storage and sharing services, is another drawback.

Huawei is an enormous company, with strengths in networking, telecom, enterprise, and IoT, but it is unclear how connected, and to what level of integration, the AnyOffice platform has with these larger solutions. Huawei must better articulate how AnyOffice fits into this larger IoT, security, and networking story.

Consider Huawei When

Consider Huawei when your organizations' operations are extensively in China and APAC, in general, and prefers an on-premise deployment of EMM. Also companies heavily invested in other Huawei technologies, from network and security infrastructure to IoT and mobile devices, should also consider the AnyOffice platform for inherent integration benefits when deployed with these technologies.

IBM

IBM is a Leader in the 2018 IDC MarketScape for EMM software. IBM's MaaS360 is a cloud-based EMM product, hosted on the company's own SoftLayer cloud infrastructure and datacenters. MaaS360 has become the most widely deployed IBM SaaS solution delivered from this platform, and it brings a strong set of mobility-focused EMM features with capabilities around UEM and IoT device support scenarios. IBM in the past year has made strong inroads with carriers and managed service providers, going to market with MaaS360-based managed mobility solutions and gaining customers in the small and midsize market — a segment difficult to reach for EMM technology deployments and expansion.

Strengths

IBM continues to provide strong analytics capabilities by integrating MaaS360 with Watson, IBM's cognitive and AI platform. This provides customers with cognitive insights, embedded into the platform, to help practitioners wade through emerging threat and vulnerability information to distill it into insights and recommendations that are relevant to an organization's deployment of MaaS360. In addition, the MaaS360 platform provides customers with analytics capabilities on app performance (for mobile apps configured with MaaS360's SDK) and also allows for viewing of best practices in terms of configuration and deployment of MaaS360 by analyzing anonymized customer data across the SaaS platform. IBM plans to extend this capability to PC apps soon.

IBM has a strong play in UEM with its BigFix Client Management system and patch management platform, used widely to manage large-scale PC deployments software maintenance tasks. MaaS360 is the future of modern unified endpoint management for all Google (Android and Chrome OS), Apple (iOS and Mac), and Windows devices (from XP to Windows 7, up to Windows 10, given MaaS360's long track record of PC management capabilities).

MaaS360 with Watson's App Approval Workflow capability provides strong security controls for vetting and approving apps to be published in the EMM platform's enterprise app store. This process involves code scanning and other inspection steps to ensure malicious or unsafe apps are not accidentally inserted into an enterprise production environment.

Challenges

IBM has less of a coherent workspace strategy than its larger competitors. It has many components of workspace — EMM/UEM, app provisioning, and access management with a more integrated offering.

IBM lacks a quick app creation and app integration component to MaaS360 — areas that would make sense, given the vendor's large presence in enterprise mobile app development and creation. IBM still has an opportunity to tie EMM closer to its mobile application development platform technologies,

which are still largely separate solution. (This would be a logical extension of its App Approval Workflow functionality.)

IBM has not capitalized on its broad solutions breadth in terms of cross-sell/up-selling into its enterprise customer base. The company's EMM revenue and customer installed base is equal to several pure-play or small EMM providers that do not have nearly the enterprise customer list as IBM. Larger enterprise software vendors with EMM solutions have done a better job in this aspect of go-to-market strategy.

Jamf

Jamf is a Major Player in the 2018 IDC MarketScape for EMM software. Jamf's EMM and UEM software exclusively supports Apple products across all device types – Macs, iOS iPhones/iPads, Apple TV, and Apple watch. The JamfPro platform is a single on-premise product (aimed at enterprises and education customers) that can manage most types of Apple hardware devices. Jamf differentiates itself from competitors by focusing specifically on this ecosystem, offering support of new Apple software updates usually on the day of any new software release – and usually ahead of competitive EMM solutions by several weeks. The company's JamfNow is a cloud-based product targeted at SMBs.

Jamf provides deep configuration and policy enforcement and advanced controls over application distribution and widespread updates of policies across multiple machines in the large enterprise – features more commonly associated with scalable enterprise Windows management systems, but for Macs. On the mobile front, Jamf is a full-featured EMM solution focused on iPhones, iPads, and Apple TV devices with MDM, MAM, and MCM capabilities. Jamf recently partnered with Microsoft to integrate with its Intune and SCCM EMM/PCLM platforms, allowing for integrated policy enforcement across Apple and Windows/Android devices supported by both platforms. Jamf is also making significant strides in expanding its cloud-based EMM customer footprint, with more than half of its customers now on its JamfNow SaaS solution.

Strengths

With its deep support of Apple, Jamf has also established strong relationships with Apple enterprise application and systems partners in the verticals in which Mac and iOS are strong – namely education, medical and hospitals, and high-tech/software companies. This has led to some advanced and unique solutions and integrations of Jamf with other vertical and horizontal software platforms, such as EPIC in the health information systems market.

Jamf has strong capabilities around Mac OS and iOS management and policy enforcement, with a unified management and administrative experience for both mobile and PC users. Policies around access control, data management, and identity can be easily applied to mobile and PC devices via the console. Among Jamf customers IDC spoke with (which all had mixed Windows/Android/Apple environments), the product's support capabilities for Mac OS/iOS/tvOS justified the use of Jamf specifically for these devices, along with another third-party EMM solution for managing non-Apple endpoints.

Challenges

Jamf does not consider it's Apple-only approach a challenge. It specifically targets Apple and differentiates on this; however, enterprises with heterogeneous mobile and PC endpoint environments and management requirements will want a broader solution.

While Jamf is an Apple-focused EMM solution, it's total feature set for iPhone and iPad management in terms of applications, mobile content, and conditional access (especially with regard to Microsoft Office 365 apps for iOS) lagged behind some of the market leaders. Other feature gaps include telecom expense management tools/integration, mobile DLP and data access control polices, or dedicated secure mobile browser capabilities.

Consider Jamf When

Consider Jamf when your organization has a large subset of Apple devices, and especially dual-Apple end users, with Mac OS PCs and iPhones. Organizations that are considering standardization on all Apple products, from Mac OS to iOS, should give Jamf a high consideration as well. Organizations with SCCM/Intune deployments looking for Mac management should also consider Jamf for filling gap in terms of Microsoft endpoint support capabilities.

Matrix42

Matrix42 is a Major Player in the 2018 IDC MarketScape for EMM software. 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 company's Silverback EMM offering supports both mobility and PC deployments and can be considered a full UEM solution covering many device types. The company also has a widely used PCLM platform with the Empirum client management product, which complements its Silverback EMM offering and provides customers a clear path to UEM integration.

Strengths

Silverback has a strong EMM feature set, including DLP support, TEM, email and enterprise app store, as well as conditional access controls.

Matrix42 has strong synergies between its Silverback and Empirum products in its Workspace Management solution, giving its customers a strong migration story for Windows 10, EMM, and modern management capabilities.

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 than leading vendors.

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 European player with difficulty to support the United States-based organizations directly. (The company does have many multinational enterprises as customers.)

Consider Matrix42 When

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

Microsoft

Microsoft is a Leader in the 2018 IDC MarketScape for EMM software. Rapid market adoption of Microsoft's Intune and Enterprise Mobility + Security (EMS) has made Microsoft among the most widely deployed EMM platforms. Integration with Office 365 productivity SaaS suite is the key differentiator for Microsoft. Intune has advanced rapidly to meet enterprise support needs across iOS and Android platforms, as well as supporting Windows 10 migrations to modern management platforms, although the company says it is still early days for this trend.

Microsoft has elevated Intune/EMS as a key platform for its overall enterprise end-user computing strategy. It has outlined a strong migration and modern management approach with the concept of co-management — the ability to support legacy and modern Windows OSs across an integrated deployments of ConfigMgr and Intune. EMS continues to provide advanced technologies such as enterprise data access rights management, cloud access security, and advanced threat analysis and analytics.

Strengths

The creation of the Microsoft 365 brand and strategy — which tightly combines Windows 10 and Office 365 with Intune/EMS — gives Microsoft a baseline competitive advantage in any customer account considering a move to modern management and integrated EMM/UEM approach to enterprise endpoints.

Co-management with Intune and Microsoft's System Center Configuration Manager is a pragmatic approach to moving existing installed bases of Windows PCs from legacy management frameworks to modern Windows OS management and policy enforcement frameworks.

The ubiquity of Office 365 as a productivity application suite in the enterprise and the integration points with Microsoft Intune/EMS offer customers strong value in terms of integrated security management and end user. Pricing is also an advantage for Microsoft, as basic EMM capabilities come free with Office 365 subscriptions, and organizations with large enterprise licensing agreements for Microsoft software can deploy the software quickly at low cost.

Challenges

Intune/EMS has limited support for other identity, cloud security gateway and cloud access security broker platforms beyond Microsoft offerings. While the full value of Intune/EMS is coupled closely with Microsoft platforms such as Azure Active Directory and Cloud App Security, enterprises frequently rely on a wider range of identity and cloud access platforms that require EMM integration.

From an UEM perspective, Microsoft has shown little interest or road map in terms of natively supporting non-Windows PC platforms such as Mac OS and the increasingly popular Chrome OS platform (although it has supported Apple iOS mobile devices for years). While it announced a partnership with Jamf for integrated Mac management with ConfigMgr and Intune, some enterprises will not be interested in bringing in another platform for UEM.

MobileIron

MobileIron is a Leader in the 2018 IDC MarketScape for EMM software. MobileIron has an extremely capable core EMM functionality and feature set including MDM and MAM. MobileIron also offers its Docs@Work solution, which provides secure content management and access control capabilities. MobileIron's architecture around the company's secure gateway, strong certificate management, and

access controls are also strong points. MobileIron recently introduced initiatives around UEM, with its MobileIron Bridge offering (to incorporate Windows 10 devices into EMM management, as well as Mac OS).

Strengths

MobileIron is among the strongest platforms for EMM, especially around security, application ecosystem support, mobile access control, and deep support of both Android and iOS platforms.

MobileIron recently partnered with Google to integrate MobileIron into the Google Cloud Commerce Platform (formerly Orbita). This integration allows MobileIron to provide security, provisioning, and management features for cloud services purchased through the Google Cloud Commerce Platform. Specifically, MobileIron Access, the company's cloud service security and provisioning offering, provides the integrated security, as well as conditional access and license management features, for cloud services purchased on the Google marketplace.

MobileIron provides its own branded Mobile Threat Management solutions, which integrates tightly with its EMM platform from a threat detection/remediation perspective. The company OEM's Zimperium technology, which is among the leading solutions in the MTM market. MobileIron is the only EMM provider with this deep level of MTM support.

MobileIron has several key certifications for its technology, including FedRAMP and NIAP Common Criteria for device management, giving it the ability to address the customers in the U.S. federal government and other regulated industries.

Challenges

MobileIron does not have a broad enterprise software product portfolio or adjacent IT solutions or customer installed base to sell into, as does most of its larger competitors. EMM is increasingly an integration-focused technology, and MobileIron approaches this requirement with strong external partnership efforts, with over 350 external platform integrations with partners. However, for organizations looking for single-source products, larger software vendors with EMM solutions and broader portfolios can have an advantage.

MobileIron's capabilities and market approach around evolving EMM capabilities, such as analytics app creation/integration, is less complete than some of its competitors.

While MobileIron still focuses on IoT-related use cases for EMM, it scaled back its ambitions in a larger EMM-focused market approach to IoT gateway management strategy.

Sophos

Sophos is a Major Player in the 2018 IDC MarketScape for EMM software. Sophos' focus in the EMM market is on midsize enterprise security deployments, coming to market with a broad range of security products, including endpoint anti-malware, network security, and data encryption/protection solutions. Sophos Mobile is the company's EMM platform and is available on-premise and via Sophos' cloud delivery platform. Sophos Mobile integrates tightly with products across its portfolio, such as VPN/UTM integration for remote access, as well as network access control systems. Sophos also has a strong story around unified policy creation/deployment for PC/mobile endpoints, as well as integrated back-end reporting and consolidated event monitoring.

Strengths

The introduction of strong UEM capabilities around Mac and Windows PC management gives Sophos EMM users options for further expanding unified endpoint and security management architectures.

Sophos Mobile is available as a component in Sophos Central, the vendor's hosted cloud solution. This allows customers to secure mobile devices alongside all other Sophos products in a web-based, unified Sophos Central admin interface.

Challenges

Sophos is behind some of the leading vendors in the EMM market in emerging technology areas, such as EMM platform analytics, quick app creation, and EMM integration with external business app platforms.

Sophos has not sold its EMM platform broadly across its installed base. While the company's overall security software product sales are in the hundreds of millions, its EMM business is only a small fraction of its total revenue.

Consider Sophos When

Consider Sophos if you are looking to consolidate all mobile and PC endpoints management and security policy enforcement. Organizations that use Sophos extensively, or exclusively, for security products and want to deploy EMM should have Sophos Mobile on a short list of vendors for evaluation.

SOTI

SOTI is a Major Player in the 2018 IDC MarketScape for EMM software. SOTI is among the few standalone EMM vendors in the market overall, with a focus on the management of ruggedized mobile devices. SOTI has wide adoption for EMM management 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 EMM offering, providing MDM, MAM, and MCM capabilities from a single code base via on-premise or could-delivered software. Adjacent products SOTI offers include a mobile remote control and helpdesk platform called SOTI Pocket Controller, which allows IT administrators to remotely view managed end-user mobile devices (similar to Windows-based remote control IT support). Also, an internally developed MADP solution — SOTI Snap — is additional offering, allowing organizations to build mobile apps specifically for deployment and management via SOTI MobiControl. 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

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 either 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 among EMM competitors, which 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 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 EMM device deployments. Larger enterprises with ruggedized/IoT needs may consider SOTI as a separate solution for those specific use cases.

VMware

VMware is a Leader in the 2018 IDC MarketScape for EMM software. VMware's AirWatch EMM product is now an integral technology within of the company's larger Workspace ONE digital workspace platform. Now called Workspace ONE Unified Endpoint Management, it is among the most aggressive in terms of pushing UEM capabilities to the broadest set of users and challenging incumbent PC life-cycle management platforms for migration to UEM and modern management. VMware also recently acquired mobile app analytics vendor Apteligent to bolster this offering through new Workspace ONE Intelligence capability that provides app analytics along with UEM analytics and automated workflows. The company also plans to integrate end-user security analytics into Intelligence from its acquisition of E8 Security.

Dell EMC, VMware's majority owner, provides the company with a strong entry point in terms of enterprise endpoint and PC market access and integration. Workspace ONE UEM is able to provide configuration and security settings across a range of devices, including Dell Chromebooks, and BIOS management on Dell PCs. It is also a key technology for enabling Dell's device-as-a-service offering.

Strengths

The ability to create specialized mobile apps and app integrations in the Workspace ONE environment, via app connectors, or custom functions leveraging the platform itself, is a strong differentiation point for the company. Line-of-business technology enablement will be a key requirement for EMM platforms over the next several years.

Workspace ONE offering ties together mobile, traditional, and virtual client computing technologies, is a differentiator in terms of total value and major cross-sell/upsell opportunity for AirWatch among VMware's overall installed base.

Workspace ONE UEM has strong features for managing Windows 10, as well as pre-10 Microsoft PC deployments and Mac and Chromebook. Support for Win32 app distribution, GPO policy enforcement, and other Windows-centric features will help the company gain traction in PCLM migration opportunities among its installed base and beyond.

VMware is gaining analytics customers and adoption of its Workspace ONE Intellgence analytics package. This is a key differentiation point for the vendor as it continues to add features and capabilities beyond traditional, core EMM features and capabilities.

Challenges

While VMware's expansion into mobile apps is ambitious, it is an area beyond the company's traditional IT operations and management market and could potentially be a stretch for the company. The mobile app development platform market is well established and mobile application creation and customization requirements could be difficult for the vendor to support, alongside its core endpoint management functionality.

While VMware has strong EMM/IoT use case support, it lacks current support for some key device OS platforms in this market, such as Linux, Android Wear, and Android Things.

Workspace ONE and AirWatch have strong enterprise presence, but have had less success addressing small and midsize customers. AirWatch plans to address this market segment more aggressively in 2H18 with new carrier and managed service provider partnerships.

Zoho

Zoho is a Major Player in the 2018 IDC MarketScape for EMM software. Zoho, a SMB- and midmarket-focused software company, has over 4,000 developers working on software products ranging from CRM to productivity apps and software development tools. The company's EMM solution, Mobile Device Manager, comes from the ManageEngine division of Zoho. ManageEngine also markets its Desktop Central platform, a complete PC life cycle, IT asset, and service desk management platform that supports mobile device and application management via an integrated feature set. Desktop Central and Mobile Device Manager can integrate tightly to provide a strong, centralized UEM solution for converged endpoint management.

Strengths

ManageEngine Mobile Device Manager supports a broad range of endpoint types, from client PCs (Mac, Windows 7–10, and legacy) to Linux. This allows ManageEngine to address a broad range of IoT and single-purpose device management opportunism while positioning its clients well for unified endpoint migration on a system that is already well integrated.

ManageEngine offers a strong single-console capability for all device management functions, including device tracking and management, configuration, and application of security and application polices.

Zoho's broad software portfolio creates many interesting opportunities for cross-selling within the Zoho customer base, as well as integration opportunities with Zoho's MADP, enterprise mobile apps, and IoT software products.

Challenges

ManageEngine does not integrate with cloud-based security or access management solutions, such as cloud-based SSO/identity platforms or CASB offerings. It also has limited mobile security vendor partnerships.

The ManageEngine platform lacks basic mobility management platform features found in market-leading EMM solutions such as telecom expense management, secure PIM and app wrapping or app, or an integrated file sync and share platform for full MCM capabilities.

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 EMM 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 EMM 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

Enterprise mobility management (EMM) is a competitive software market that pulls revenue from various enterprise systems management, security, and content management markets. EMM offerings include capabilities that enable the secure management of devices, applications, and content within a mobile computing context.

A mobile device management (MDM) solution includes many of the standard features included in PC management solutions but also additional functionality that addresses the unique needs of mobile devices such as smartphones and tablets. In its current incarnation, the EMM software market is not meant to capture the entire IoT device management opportunity; however, a portion of the IoT device management market may be included where existing EMM vendors broaden out their platforms to support additional device types. Some of the key features of a mobile device management solution are:

- Device provisioning and management configuration settings
- Inventory/asset management
- Software distribution (applications, OS, and firmware updates)
- Remote wipe/lock and remote control for systems diagnostics
- Policy/compliance management (encryption management, device posture, etc.)
- Authentication and certificate management
- Real-time device monitoring, location information, and GPS tracking
- Reporting and analytics on devices

Mobile application management (MAM) refers to a solution by which specific mobile applications can be managed, secured, and distributed by IT organizations and that typically allows for enhanced policies to be applied to individual applications or a grouping of apps. Mobile application management solutions can either supplement MDM functionality or function as standalone offerings. Common functionalities included within MAM include enterprise app storefronts, containers, and app wrapping.

Mobile content management (MCM) solutions for the enterprise provide IT with a secure way to provide access to files/content/data sitting in various data stores to mobile devices. Such solutions may also provide mechanisms to securely collaborate on this content. These products allow IT to manage who gets access to what information and may tie in with other back-end or mobile-specific policy systems. Preventing data loss is a key goal of these products, and they do so by providing IT with a mechanism to control data flow in and out of the secured app and secure communication between apps. These solutions assist with compliance and governance by offering reporting on user activity with mobile content. Mobile content management solutions may be either cloud based or on-premise based and may also provide access to content that is in the cloud or behind the firewall.

Strategies and Capabilities Criteria

Tables 1 and 2 provide key capability and strategy measures, respectively, for the success of enterprise mobility management platform vendors.

TABLE 1

Key Capability Measures for Success: Worldwide Enterprise Mobility Management Software

Capabilities Criteria	Definition	Weight
Customer service delivery/offering/ satisfaction	The vendor's customer-facing delivery capabilities satisfy market wants and create a strong level of value for its customers.	10.00
Functionality or offering	The vendor's capabilities maximize the connection between offerings and customers, such as delivery, partnerships, pricing, distribution, marketing, sales, and service.	50.00
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.	15.00
Pricing model or structure of product/offering	The vendor is willing to demonstrate value through flexible pricing mechanisms, including profit sharing–based relationships.	7.00
Range of services	Current offerings match directly to current customer needs to deliver maximum customer benefit.	11.00
Cost of ownership	The product provides customers with strong TCO capabilities due to inclusiveness of features and functions, reduction/savings in operational/acquisition costs, and overall value.	7.00
Total		100.00

Source: IDC, 2018

TABLE 2

Key Strategy Measures for Success: Worldwide Enterprise Mobility Software

Strategies Criteria	Definition	Weight
Delivery	The delivery model for the product, as well as associated support and maintenance services is well positioned for future customer needs, and it aligns with market trends.	23.00
Financial/funding	The company will generate, attract, and manage capital well over the next three to five years to create market value.	9.00
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.	24.00
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.	35.00
Innovation	Strategies to grow the business are aligned with market trends and future opportunities over the next three to five years.	3.00
R&D pace/productivity	The pace of continued investment is expanding the company's industry cloud offerings over the next three to five years.	6.00
Total		100.00

Source: IDC, 2018

LEARN MORE

Related Research

- *IDC Innovators: Unified Endpoint Management Software, 2018* (IDC #US43983917, June 2018)
- *Worldwide Enterprise Mobility Management Software Market Shares, 2017: Evolving Mobility Use Cases Drive Market Growth* (IDC #US43293918, May 2018)
- *Worldwide Unified Endpoint Management Software Forecast, 2018-2022* (IDC #US43293818, May 2018)

Synopsis

This IDC study represents a vendor assessment of providers offering enterprise mobile mobility management (EMM) software through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for EMM software. The evaluation is based on a comprehensive and rigorous framework that

assesses how each vendor stacks up to its peers, and the framework highlights the key factors that are expected to be the most significant for achieving success in the EMM market over the short term and the long term.

"EMM is now seen as a strategic platform for managing a wide range of enterprise endpoint computing devices, and the apps and data these endpoints access," says Phil Hochmuth, program director, Enterprise Mobility Research at IDC. "Unified endpoint management – combining mobile management functions with PC and laptop client devices – is an emerging requirement for EMM platforms. EMM software is also extending into some IoT device management use cases, where smart connected devices run standard mobile operating systems."

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

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com