

## IDC MarketScape

# IDC MarketScape: Worldwide Unified Endpoint Management Software 2019-2020 Vendor Assessment

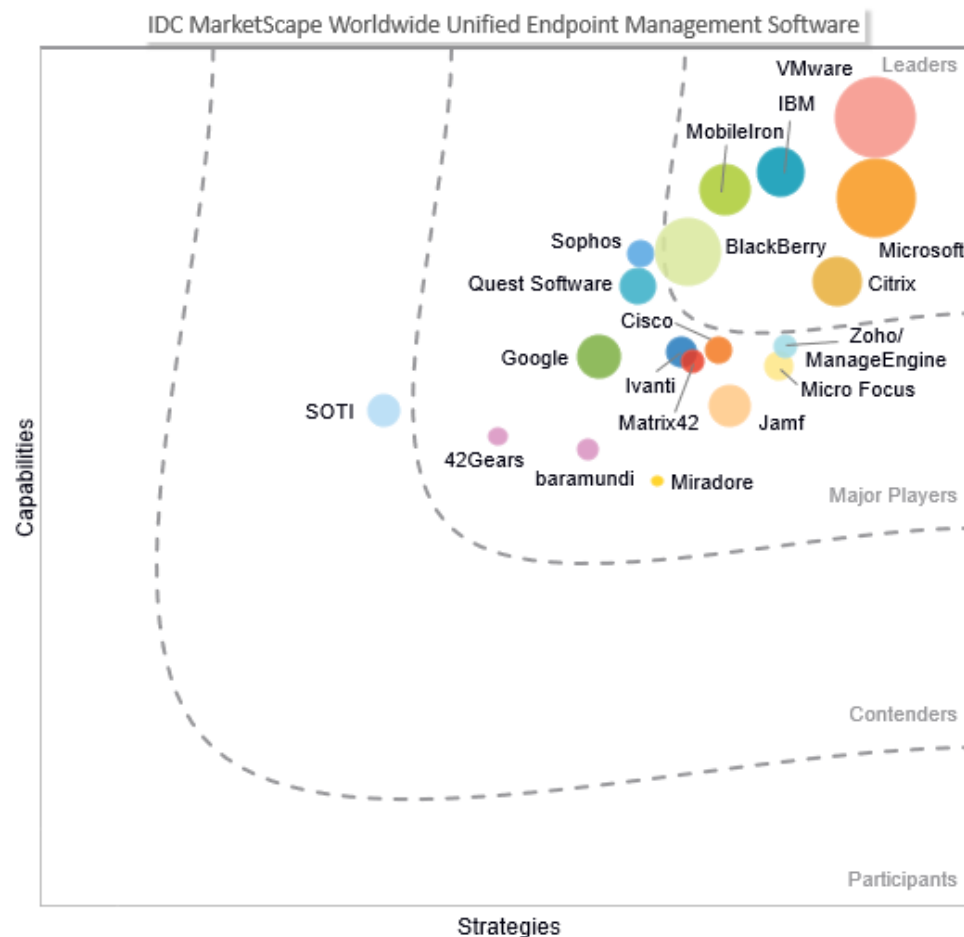
Phil Hochmuth

THIS IDC MARKETSCOPE EXCERPT FEATURES BLACKBERRY

## IDC MARKETSCOPE FIGURE

**FIGURE 1**

### IDC MarketScape Worldwide Unified Endpoint Management Software Vendor Assessment



Source: IDC, 2019

## IN THIS EXCERPT

The content for this excerpt was taken directly IDC MarketScape: Worldwide Unified Endpoint Management Software 2019-2020 Vendor Assessment (#US45355119). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

## IDC OPINION

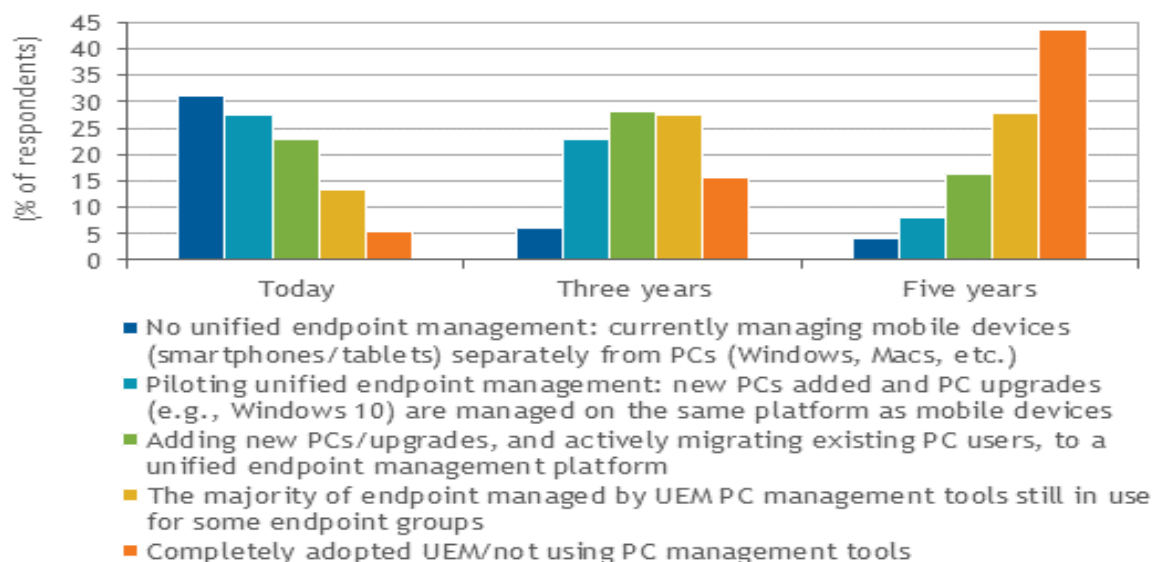
Unified endpoint management (UEM) is the convergence of mobile and PC device management, as well as additional endpoint and network-connected device types, in an enterprise IT architecture. The modernization of endpoint operating systems – from the introduction of smartphone platforms such as iOS and Android to Windows 10 and the latest macOS 11 Catalina, as well as Chrome OS – has introduced more streamlined, cloud-centric device management, software distribution, and configuration/policy enforcement frameworks. This now makes it possible to manage five or more broadly used device types via a single management software product or connected suite of products.

UEM is an inevitability in most enterprises. According to IDC's 2019 *Enterprise Workspace and Mobility Decision Maker Survey*, only 31% of enterprises have *no* UEM initiatives currently going; the other 69% are at various stages of UEM adoption, from small pilots to pushing UEM through at scale with new Windows 10 upgrades. By 2024, 72% of enterprises expect to be either 100% on UEM or having the majority of endpoints managed by the technology (see Figure 2).

FIGURE 2

### Unified Endpoint Management Adoption Plans

Q. Thinking of how your organization manages all endpoint devices, what is the state of unified endpoint management today and how will this look three and five years from now?



Source: IDC's *Enterprise Workspace and Mobility Decision Maker Survey*, 2019 n=500

IDC sees UEM as a cornerstone technology for business building intelligent managed digital workspace environments for employees. These workspaces can range from traditional offices to field-based work, task-oriented roles as well as specialized environments integrating multiple device types. These modern, connected workspaces will also generate valuable data – not just in terms of the data and apps workers use and access but also data "chaff" or "exhaust" of the systems and devices themselves. As organizations move to modern device OSs and modernize the management infrastructure supporting these devices, the collection of this endpoint data and the use of analytics will help organizations become more secure, optimize workforces and business operations, and drive employee satisfaction and engagement in digitally transformed businesses.

This study is the second in a series of four IDC MarketScape research studies and considers key capabilities and strategies required for success in the unified endpoint management market. Vendors with offerings in the UEM market provide this breadth of capabilities today with product development road maps that will match future needs. Key findings include:

- There are two distinct camps of enterprises competing in the UEM segment of the enterprise mobility management (EMM) market – modern management-focused EMM vendors looking to expand device enrollment to PCs and traditional PC life-cycle management (PCLM) vendors that have added mobility management to their offerings to have more inclusive endpoint device management capabilities and to compete with EMMs looking to enter the PCLM market.
- 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. macOS 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

---

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 for at least one mobile operating system (e.g., iOS, Android), as well as integrated, single-product support for at least one of the following PC OSs: Windows (7/10), macOS, Chrome OS, or Linux
- EMM product revenue of \$5+ million for calendar year 2018 (Revenue was estimated in April 2019 and may differ from forthcoming market 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, CA Technologies, Kaspersky Lab, Kony, Prey Software, Samsung SDS, and Symantec.

## ADVICE FOR TECHNOLOGY BUYERS

---

This study analyzed and rated vendors across a broad range of criteria regarding capabilities and strategies in the UEM market. Technology buyers should evaluate UEM platforms with a holistic view of current and endpoint device management requirements and future goals for enabling modern end-user computing enablement. 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

- **Strong UEM capabilities and road map for customer success.** While UEM 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 critical for management with UEM. Critical support issues will involve transitioning Group Policy Object (GPO) and PC image management frameworks and modernizing patching and software distribution to UEM-based modern management.
- **Core EMM/MDM support.** In addition to PC support, core mobility functionality of UEM platforms is 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 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 endpoint security, identity, IT service management, IT asset management, VPN, network access control (NAC), network infrastructure, mobile devices, mobile applications or app development platforms, virtualization, and data/analytics capabilities all have relevant ties with UEM platforms.
- **Adjacent mobile security integration.** With the increased focus on mobile security and the endpoint, UEM vendors that support integration with a broad set of mobile threat management (MTM), endpoint security, security information and event management (SIEM), 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, 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.
- **Capabilities for supporting noncorporate devices or BYOD users.** Support for employees' personal mobile device, or BYOD, is critical to expanding seats and overall management scope of an UEM 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 devices.
- **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 OS that is out of date).

- **Scalability and cloud-based delivery capabilities.** Cloud is the future of the UEM market as most vendors offer some level of this delivery model. SaaS-based UEM fits with the mobile/cloud synergies of enterprise mobile computing, allowing businesses to flexibly deploy UEM 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 UEM as many organizations still require some on-premise deployment scenarios, particularly security-sensitive industries such as financial and government or in deployments in European Union countries with more stringent cloud data privacy regulations.

## 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.

### BlackBerry

BlackBerry is positioned in the Leaders category in the 2019-2020 IDC MarketScape for UEM software.

BlackBerry's EMM/UEM product, BlackBerry Unified Endpoint Manager (BlackBerry UEM), covers a wide range of mobility, PC, and IoT/ruggedized endpoint management use cases and deployment scenarios, with a strong focus on data and hardware security. In BlackBerry's refocused strategy as an enterprise system infrastructure software provider (post-exit from the smartphone market), security continues to be a strong focus area in terms of standalone products and product feature integrations. (The company's AtHoc emergency management/notification software and Secusmart call encryption technology, as well as the company's hardware-based security capabilities in the embedded QNX OS and its Certicom product line, all fall in this category.) However, the company made a \$1.2 billion investment in security with its 2018 buyout of Cylance – an independent endpoint and cloud security technology provider focused on advanced threats, behavior-based security detection, and other next-generation security capabilities. The company has already made interesting integrations of Cylance technology into its UEM offering, with a conditional access control offering that blends Cylance's AI-based threat detection with BlackBerry UEM access control features. The company plans to further integrate Cylance technology across its entire portfolio while still maintaining the company as a somewhat separate, competitive security provider. BlackBerry's Radar cloud-based transportation/logistics tracking solution and the Spark IoT communications platform are adjacent technologies and markets where BlackBerry can both cross-sell UEM and security solutions and provide integrated platforms/offerings.

### Strengths

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.

With Cylance, BlackBerry now has a complete endpoint management/security technology portfolio matched by only a few other vendors in the market. As enterprises continue to integrate and converge all end-user computing management and security functions, with UEM and integrated endpoint security, BlackBerry will be in a good position to cross-sell the BlackBerry-Cylance customer base and

offer a converged endpoint management/security story. There is strong potential for extending these security and threat intelligence capabilities into the IoT and embedded/connected endpoint management markets BlackBerry serves (e.g., QNX).

With Cylance, BlackBerry has an extremely diverse ecosystem of integration and resale channel partners, ranging from security-focused solution providers, distributors, VARs, and SIs, and nearly every major mobile carrier in every region worldwide. BlackBerry has built a strong portfolio of supporting and adjacent enterprise end-user computing access and security technologies around UEM, including BlackBerry Access, a secure browser-based remote access control solution for providing secure web application access to behind-the-firewall IT resources.

BlackBerry has strong Microsoft integration capabilities with its Enterprise BRIDGE solution for securing/managing Microsoft Office365 apps in the BlackBerry Dynamics security container architecture as well as applying policies to O365 apps via Microsoft Graph API.

## **Challenges**

BlackBerry's presence in terms of installed base for UEM for PC management is smaller than that of other prominent UEM vendors. The company also has fewer capabilities around "traditional" PC management functions – GPO support/translation, system imaging/management, and software distribution.

BlackBerry has a strong presence in industries such as banking, U.S. and international governments, medical, and other highly regulated/security-focused markets; however, it has a smaller presence in industries traditionally less invested in overall risk and security.

## **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 software and SaaS solutions provide change, configuration, compliance, asset tracking, and software distribution for client, desktop, mobile devices, and some IoT devices (e.g., devices and systems with which employees, customers, or others interact, input/retrieve information). UEM solutions also manage some peripheral hardware and software assets but not network devices, storage, or server systems. UEM includes technologies and products previously classified as PC life-cycle management, as well as IT asset management relating to end-user computing devices. UEM solutions also include some software distribution functions relating to end-user and endpoint applications – fixed/mobile PC, mobile device (e.g., smartphone/tablet), and some IoT endpoint devices relating to end-user device operating systems and software. Mobile device management and configuration technologies also fall under the UEM umbrella. Extended functions of solutions in enterprise mobility management (EMM, an IDC competitive market) such as network security, security and vulnerability management, mobile content management/security, and remote access are not part of the UEM functional market.

## LEARN MORE

---

### Related Research

- *Worldwide Enterprise Mobility Management Software Forecast, 2019-2023* (IDC #US43897319, September 2019)
- *2019 U.S. Enterprise Mobility and Workspace Management Software Survey* (IDC #US45518219, September 2019)
- *Worldwide Enterprise Mobility Management Software Market Shares, 2018: A Market Transitioning to Unified Endpoint Management* (IDC #US43897519, June 2019)

### Synopsis

This IDC study represents a vendor assessment of providers offering unified endpoint management (UEM) 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 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 UEM market over the short term and the long term.

"End-user computing device environments are diversifying as employees continue to bring personal devices into work environments, but also as enterprises expand and grow their use cases for mobile and PC deployments," says Phil Hochmuth, program vice president, Enterprise Mobility and Client Endpoint Management, IDC. "In the face of increased endpoint heterogeneity, enterprises are moving toward converged management frameworks, and UEM in particular, to reduce staff, tools, and costs and centralize policy and security controls."



## 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

---

### Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2019 IDC. Reproduction is forbidden unless authorized. All rights reserved.

