IDC MarketScape

IDC MarketScape: Worldwide Unified Endpoint Management Software 2022 Vendor Assessment

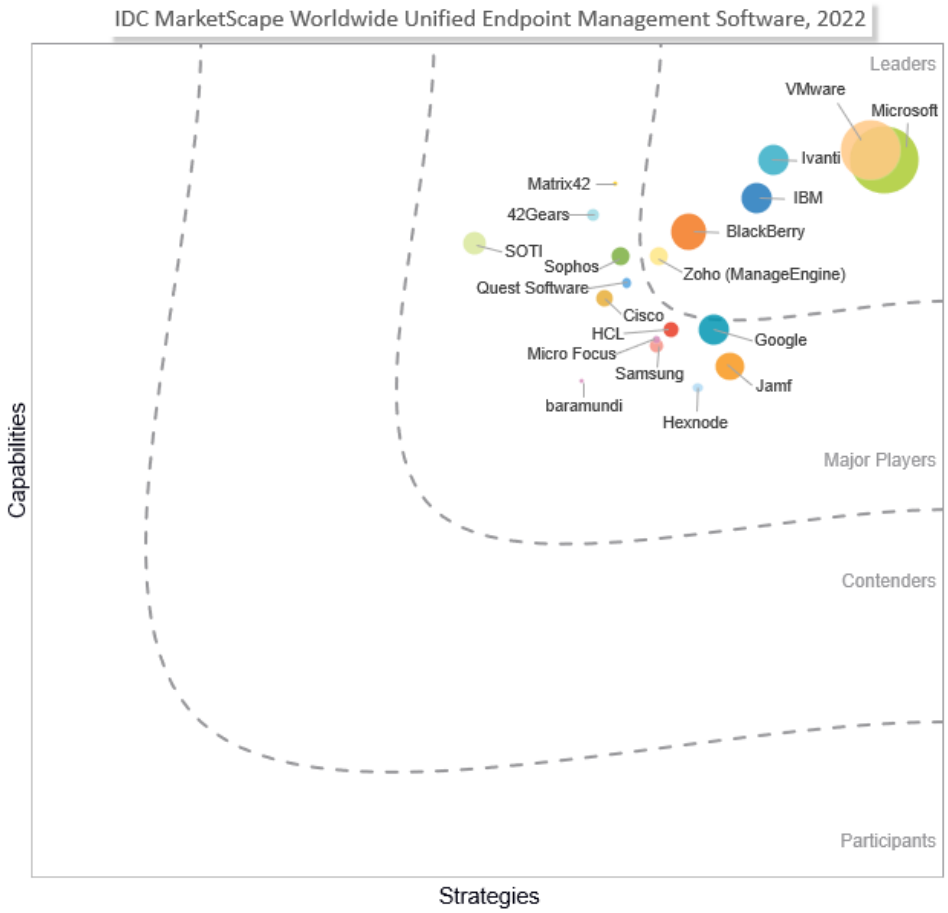
Phil Hochmuth

THIS IDC MARKETSCAPE FEATURES BLACKBERRY

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Unified Endpoint Management Software Vendor Assessment



Source: IDC, 2022

May 2022, Excerpt of IDC #US48325122

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

IN THIS EXCERPT

The content for this excerpt was taken directly IDC MarketScape: Worldwide Unified Endpoint Management Software 2022 Vendor Assessment by Phil Hochmuth (Doc #US48325122). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Advice for Technology Buyers, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

As enterprise IT operations start returning to some form or pre-COVID-19 pandemic version of "normal," organizations are discovering new use cases and requirements for their endpoint device management platforms. It is now critical for unified endpoint management (UEM) technology to be able to support multiple device types accessing corporate data, apps, and IT resources both on network (attached to a corporate LAN, an extended WAN, or via a VPN connection) and off network (connected to the public internet via wired/wireless broadband, but not attached to private business networks).

In addition, it is important for UEM platforms to address specific business use cases and tactical workflows and operations. Mobile devices, tablets, and laptops are now used broadly in task-specific scenarios (e.g., retail, optical data input/capture, logistics record keeping, public safety communications) that may require different features and capabilities from a device management perspective compared with standard end-user computing requirements for mobiles or PCs. In some instances, enterprises may choose multiple UEM platforms, deploying technologies in best-of-breed scenarios to handle various use cases across the organization.

Customer UEM and device management requirements will also vary widely based on organizational details (enterprises versus SMBs, vertical market or region, etc.). Also, decisions on device-type standardization (e.g., Mac-only or Windows-only shops, Android-centric firms, or iOS-only deployments) will also largely dictate the type of UEM technology adopted.

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 PCs and laptops as well as for mobile devices (smartphones and 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:

- **Hybrid worker device support scenarios key.** The UEM platform should be able to support endpoint device management from both an on-premises/in-office perspective and a remote or work-from-home scenario, with full support functionality across both scenarios.
- **Strong UEM capabilities and road map for customer success.** While UEM platforms today mostly manage smartphones and tablets, laptops and PCs (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.
- **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.
- **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).
- **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.
- **Capabilities for supporting noncorporate devices or bring-your-own-device (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.
- **Ability to address three to four major endpoint device operating systems.** To be a viable UEM platform, an offering should support at least three of the four major operating systems for an enterprise endpoint device (Windows, macOS, iOS, and Android) and be able to support both mobile and PC form factors across these OSs.

VENDOR SUMMARY PROFILE

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 strengths and challenges.

BlackBerry

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

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.

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).

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. 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.

"Enterprises are emerging from the pandemic with new requirements around how endpoint devices are used, deployed, managed, and secured," says Phil Hochmuth, program VP, Endpoint Management and Enterprise Mobility at IDC. "Unified endpoint management adoption was strong through the

pandemic, but what has emerged is a market where multiple platforms may now exist in an organization that focuses on unifying endpoint management for specific use cases. Deploying one UEM tool to 'rule them all' is becoming a rarer thing in most deployments."

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