IDC MarketScape: Worldwide Unified Endpoint Management Software 2021 Vendor Assessment
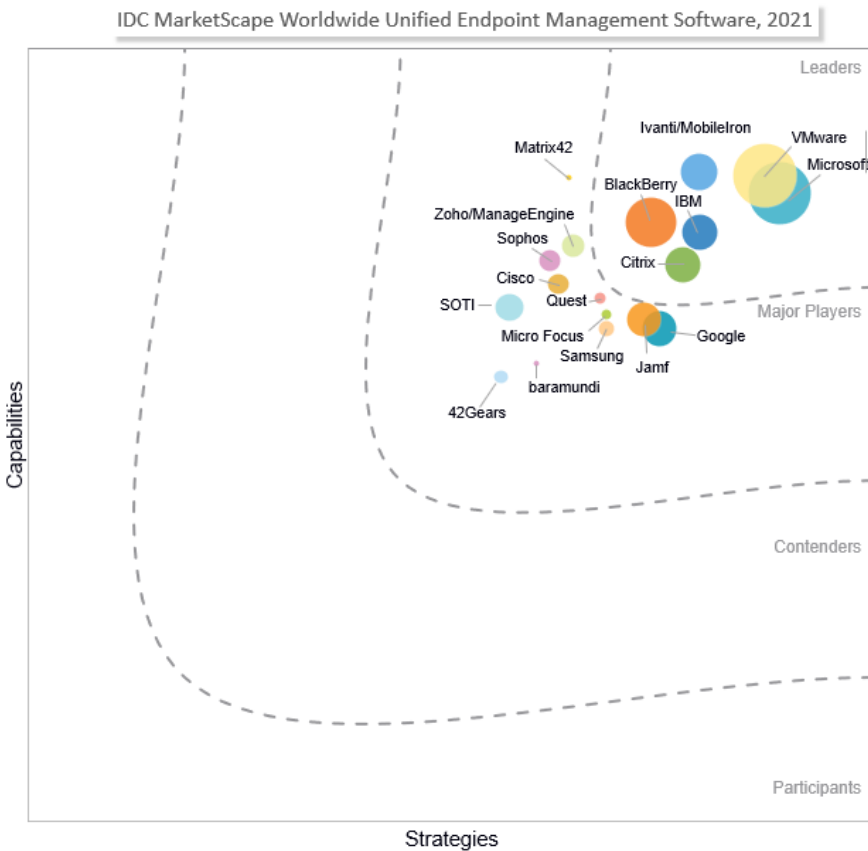
Phil Hochmuth

THIS IDC MARKETSCAPE EXCERPT FEATURES VMWARE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Unified Endpoint Management Software Vendor Assessment

IDC MarketScape Worldwide Unified Endpoint Management Software, 2021

Source: IDC, 2020
Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Unified Endpoint Management Software 2021 Vendor Assessment (Doc # US46957820). 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

Among enterprises, the management of endpoint computing devices – PCs, laptops, smartphones, tablets, and so forth – is rapidly converging around the concept of unified management. This is the provisioning, configuration, management, monitoring, and maintenance of up to five different operating systems (OSs) (Windows 10, macOS, iOS, Android, and Chrome OS) via a single console or software tool. Nearly three-quarters (72%) of U.S. enterprises are piloting or fully deploying UEM solutions currently, with 45% of firms beyond the pilot stage, according to IDC's 2020 *Enterprise Mobility Decision Maker Survey.* But any technology convergence or transformation effort has a long tail of partial integration and various states of hybrid management (think of the TDM/VoIP convergence of the early 2000s or cloud migration in the 2010s). Endpoint management convergence will be similar; in five years, fewer than half of enterprise IT leaders expect to be managing all endpoints solely with UEM technology.

The long tail of hybrid/legacy device management means co-management – applying policies to devices via a modern UEM and legacy PC life-cycle management (PCLM) tools – will be the norm in many firms. Some endpoint management leaders won't rewrite or throw out years of finely honed scrips and custom configuration options not supported (or easily replicated) in modern UEM software. However, some firms starting IT operations from scratch will adopt UEM out of the gate, choosing modern/cloud-managed and provisioning endpoint approaches. Owing to the COVID-19 pandemic, and expanded remote/work-from-home workforces, many firms are quickening their UEM migrations and modern endpoint provisioning and management. (Most UEM and modern management solutions can affect via the internet/public cloud, without requiring or taxing enterprise VPN and network resources.) To that end, spending on UEM solutions will be a priority among firms in the United States and worldwide going into the new year, as more than one-third of firms say they plan to increase spending on this technology in 2021 (source: IDC's *COVID-19 Impact on IT Spending Survey,* conducted during the October 15–30, 2020, period).

This study is the first in a series of IDC MarketScape documents evaluating product offerings from over 18 vendors worldwide. This study focuses on UEM solutions holistically, with considerations for the broadest set of deployment scenarios and requirements. But not one UEM solution fits all use cases. Subsequent documents will look at specific requirements and evaluation products based on criteria focused on the following areas: UEM solutions for small and midsize businesses, UEM for ruggedized device and IoT deployments, and UEM solutions for Apple device management.

For this study, IDC analyzed offerings from 18 different vendors and interviewed over 30 customers using UEM products. Key findings for this study include:

- Most enterprises are using multiple UEM solutions for various use cases and/or regional support strategies.
- Convergence of teams comes before the single pane of glass: most end-user organizations.

- Support of five endpoint platforms (Windows, Mac, Apple, Android, and Chrome OS) is common among most vendors in the market.
- Endpoint analytics and advanced telemetry gathering and analysis is a growing offering component among many forward-thinking UEM solutions providers.
- Many vendors are positioning UEM as an infrastructure/security component to a larger "workspace" strategy around how end users work and interact with digital technology.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC invited vendors to participate 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 2019. Revenue was estimated in May 2020 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 UEM market with relative products that did not meet the vendor inclusion criteria for this study. These companies include Addigy, Amtel, HCL Technologies, Hexnode, Kandji, Prey Software, and Verizon.

ADVICE FOR TECHNOLOGY BUYERS

- **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 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.
- **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.
- **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.

- **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-premises servers and supporting IT resources. Hybrid is still an important aspect of UEM as many organizations still require some on-premises 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 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 the vendor's strengths and challenges.

VMware

VMware is positioned in the Leaders category in this 2021 IDC MarketScape for worldwide UEM software. VMware Workspace ONE is the vendor's main UEM offering, which also combines elements of desktop virtualization, endpoint and application analytics, as well as security and identity into a single brand/platform. As an UEM platform, Workspace ONE covers a broad range of device types (from major end-user device platforms to more specialized IoT and ruggedized endpoints). The company has also made a concerted effort to expand its traditional mobile installed base to more Windows and Mac devices, with specific focus on helping legacy-managed Windows 10 devices move to modern or a co-management state.

In 2020, Workspace ONE broadened its scope extensively into security. With the Carbon Black technology, VMware has integrated anomaly detection alerting into the platform, where user behaviors that deviate from baseline normal measurements can be flagged (via the Carbon Black AI technology) for deeper inspection by IT or security teams. Security functionality has also been extended to support more home/remote use cases with Workspace ONE Tunnel, which turns anomaly detection capabilities into a continuous authentication/verification function, quarantining or blocking users based on detected anomalies or conditions of the end-user device state not deemed secure enough.

VMware is also looking to expand Workspace ONE functions to nonmanaged Windows 10 (i.e., BYOD laptops in home offices) or Windows PCs managed by other third-party/legacy PCLM platforms. Intelligent Hub is the main user-facing app for Workspace ONE, which aggregates apps and overall

workspace. Intelligent Hub is now deployable on Windows 10 devices not managed by VMware's UEM solution. Similar to container-like technology deployed on BYO mobiles, this allows an unmanaged/third party-managed PC to securely access Workspace ONE managed/provisioned apps and services without having to manage the underlying PC OS.

The company also expanded its automation and app-development/creation workflow capabilities with Freestyle Orchestrator – a tool aimed at IT admins for creating management orchestration workflows (such as automating tasks around multiple-device onboarding and configurations, multistep patching, or software updating). This complements the existing Mobile Flows function of Workspace ONE, which allows end-user-created quick tasks and workflow integrations to other enterprise app platforms, using the Workspace ONE email client as the main UI.

Analytics, from a security standpoint but also for end-user productivity, worker satisfaction, and experience monitoring, was another expansion area for Workspace ONE. Employee Experience Score is a feature that aggregates multiple telemetry points from managed devices, users, and aggregated activity and provides IT administrators and business leaders with data on the experiences users are having with IT systems and technology as a whole. Data on app performance and crashes, device-level metrics (slow boot times, hardware failures), and other metrics on app usage and access trends are available in dashboards and reports, which can be consumed by IT or other business units or lines-of-business leaders.

Strengths

Workspace ONE supports all major mobile provisioning and enrollment services, including Windows Autopilot, Apple Business Management device enablement (formerly DEP), Android Enterprise Zero-touch, and Samsung Knox Enrollment.

VMware has expanded its capabilities around macOS management support, with extensive support for Mac management features such as agent-based management, advanced scripting functions, OS and third-party app patching, and device and software inventorying of Macs. Vulnerability management and alerting functions are also being extended to Mac via Workspace ONE, as well as the Employee Experience Score function for macOS users.

VMware continues to offer strong support for frontline, IoT, and ruggedized device use cases with Workspace ONE, including support for Apple devices in: iOS User Enrollment for separating underlying device management from role-based app/data management and shared iPad for Business support, which allows multiple or "shift" workers to log in and out of a single iPad while maintaining individual data/settings management (such as in iPad retail POS scenarios). Workspace ONE also supports Android Enterprise Kiosk, Single App Mode, and the corporate-owned single use profile, as well as the Samsung Knox and DeX technologies for device lockdown and PC integration/extension.

VMware's Workspace ONE Express and Workspace Express+ were fine-tuned in 2020 to better address SMB market requirements, including low per-device pricing; preconfigured blueprints, workflows, and automations for SMB users (such as device deployment/deprovisioning, app delivery/life-cycle management); and other features targeting small or nontechnical teams managing mobility and endpoint management.

Challenges

With its Mobile Flows and Freestyle Orchestrator, VMware is inserting more automation and service functions into its UEM solution. However, the company lacks formal integration and support of third-

party IT service management tools (beyond ServiceNow and Atlassian). To some extent, the tools VMware is building into Workspace ONE may compete with or overlap with ITSM tools that customers may already have in place.

With over a year since the acquisition of Carbon Black, VMware has integrated elements of the security technology, specifically AI anomaly and threat detection, into its broader UEM offerings. However, there have to date no deep levels of product integration that end users might have expected (i.e., endpoint security built into Workspace ONE or other VMware end-user computing technologies offered by VMware). To some extent, Carbon Black still operates like a separate company, which is somewhat by design in order for VMware to maintain broader security partnerships and to support customers.

Consider VMware When

With its support for a broad set of UEM use cases, VMware should be considered by organizations looking to consolidate multiple aspects of end-user computing management into a singular workspace solution (including virtual desktops and apps, device management, and end user-enabling software creation).

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

- *Worldwide Unified Endpoint Management Software Forecast, 2020-2024* (IDC #US46460520, September 2020)
- *IDC TechScape: Worldwide Intelligent Digital Workspace, 2020* (IDC #US46763120, August 2020)
- *Worldwide Unified Endpoint Management Software Market Shares, 2019: Endpoint Management Convergence Drives Market Growth* (IDC #US45173520, June 2020)

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 moving away from specialization of endpoint device management – from a separate tools and IT personnel perspective – when it comes to general end-user computing use cases and workloads," says Phil Hochmuth, program vice president, IDC's Enterprise Mobility and Client Endpoint Management. "Many organizations see UEM as part of a larger strategy to streamline end-user experiences with technology across various device form factors and use cases."

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