IDC MarketScape

# IDC MarketScape: Worldwide Unified Endpoint Management Software 2024 Vendor Assessment

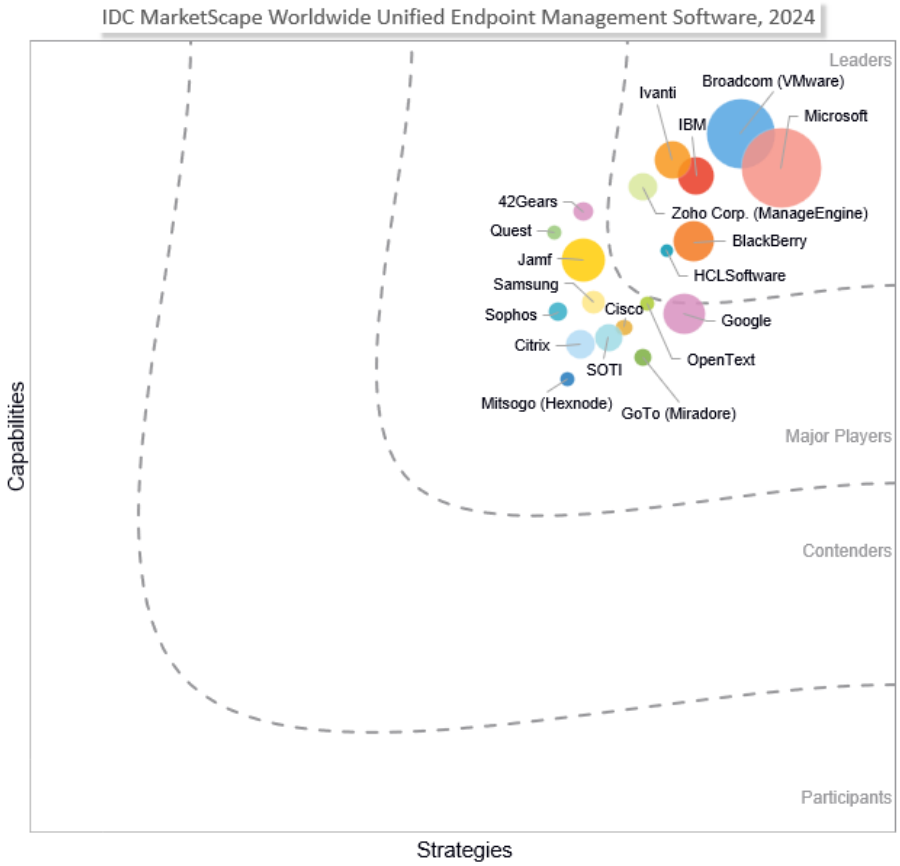
Phil Hochmuth

**THIS IDC MARKETSCAPE EXCERPT FEATURES MICROSOFT**

## IDC MARKETSCAPE FIGURE

## FIGURE 1

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




Source: IDC, 2024

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

April 2024, IDC #US51234224e

## IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Unified Endpoint Management Software 2024 Vendor Assessment (Doc # US51234224). 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

Since the unified endpoint management (UEM) market evolved from the enterprise mobility management (EMM) market in 2018 — unifying PC and mobile device management — the industry has learned that a single UEM platform is unlikely to rule across all device management use cases. According to IDC's 2023 *Enterprise Device Management Survey,* more than 70% of enterprises that have deployed UEM tools have at least two products in their environment. (More than one-third of firms have three or more UEM products in production.) While the market share in UEM is consolidating among a few top vendors, there are still dozens of established vendors, as well as new market entrants, with capable products and viable business models yielding customer success and growth. This is because UEM deployments have evolved into multivendor scenarios, with various software products targeting specific device or operational use cases. For example, knowledge workers, retail employees, delivery drivers, hospital staff, first responders, and factory workers all use PCs and mobile devices in daily activities, but in very different ways, and often with widely different types of devices. The ongoing deployment, provisioning, configuration, and life-cycle management of these digital tools often goes to UEM platforms best suited for the operational use case.

This is not to say converging all endpoint management under a single UEM isn't achievable. Many enterprises, and small and medium-sized businesses (SMBs) especially, are moving toward this goal to reduce vendor cost and multiconsole management complexity and to move to the proverbial "single pane of glass" for controlling all corporate devices. Many UEM platforms are fit for this purpose. This end goal is certainly achievable for many enterprises by considering the solutions from the 19 vendors in this IDC MarketScape.

To that end, the aim of this document is to provide detailed evaluation of the 19 capable and relevant vendors offering UEM software products for enterprises. Key features, capabilities, and strategies for these vendors and their products were analyzed with several new trends and requirements emerging in the market. These include:

- It is critical that UEM tools integrate and interoperate with key enterprise system infrastructure software (SIS) systems — especially security platforms such as identity, security information and event management (SIEM), and endpoint security tools (the top 3 UEM integration requirements cited by enterprises in IDC's 2023 Enterprise Endpoint Management Survey). IT service and asset management, client virtualization, IT operations management, and line-of-business apps and platforms are also key integration points for UEM tools.
- Increasing end-user satisfaction with technology is a top 3 driver for UEM deployment; UEM tools should include features and functions for measuring digital employee experiences (or DEXs) with devices, applications, and software platforms.
- UEM tools must be able to coexist, integrate with, and support other client endpoint management tools (e.g., patching and remote monitoring and management, as well as other UEM tools in use in an enterprise IT environment).
- While support for PC/laptop, smartphone, and tablet devices is still a baseline requirement for UEM tools, businesses are increasingly looking to incorporate more endpoint types into the

UEM fold, including wearables (watches, AR/VR headsets) and office, workspace, and facility IoT devices (digital signage, kiosks, conferencing/collaboration devices, etc.).

## IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

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

- The vendor has a unified endpoint management software product capable of managing PCs/laptops as well as for mobile devices (smartphones and tablets).
- The vendor has an estimated UEM product revenue of $5+ million for CY23. Revenue was estimated in February 2024 and may differ from forthcoming market share documents.

## 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:

- **Multidevice, work-from-anywhere users are now the norm.** UEM products must support multiple devices attached to a single user in a coordinated and well-orchestrated manner, allowing for more seamless productivity, proactive help desk support, granular device telemetry and analytics, and advanced security scenarios such as conditional access. Awareness of the user and the context of their work are key in this context.
- **Modern management is the future of device management.** Management of corporate PCs and mobile devices is converging around a singular protocol concept — mobile device management (MDM) protocols. While operating system (OS) vendors and device OEMs have implementation of MDM protocols, the central premise and end goal is the same: stateless, location-agnostic, and agentless management, configuration, provisioning, and life-cycle control over the endpoint. While agent-based device management is still necessary in many scenarios, UEM buyers should look to vendors that adhere to the principles of MDM protocol support, with the focus of their development on that support model.
- **Multi-UEM is not an oxymoron; there may not be one UEM to rule them all.** According to IDC's 2023 *Enterprise Endpoint Management Survey,* over 70% of enterprises worldwide have at least two endpoint device management tools in their environment. UEM products, by definition, must be able to manage multiple device types and form factors (laptops, phones, tablets, etc.) and across multiple operating systems (e.g., Windows, macOS, iOS, Android). This doesn't mean UEMs must be able to manage every device in every use case or scenario. Some tools are better than others, and many IT organizations choose to deploy specific UEM tools for use cases in which the tool is the best fit. Some efficiency and cost savings may be lost in supporting multiple tools.
- **End-user analytics and digital employee experience are the future of UEM platforms.** With a comprehensive view of a worker's devices, UEM platforms are positioned to collect, analyze, and take action on volumes of available data on the state of an end user's digital experience. Employee behavior, device and application health, and usage patterns based on location, time of day, network type, and so forth are all critical in better understanding how employees work with the devices and apps they are given to do work. UEM tools are at the vanguard of providing capabilities around data collection, analytics, and reporting to be part of a larger DEX initiative spearheaded by UEM technology.
- **Conditional access controls and policy enforcement are table stakes.** 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 or health of the device being used (from the standpoint of a jailbroken/rooted device or an operating system that is out of date).

- **Specialty use device scenarios — frontline workers, multiuser endpoints, field workers, and deskless workers — must be considered.** UEM tools must be able to support management of devices across nontraditional use cases (e.g., beyond basic mobile computing: voice/video calls/meetings, email, calendar, messaging, and productivity tools). Device support for frontline workers, users or ruggedized endpoints, and field workers should be as extensible as standard UEM device support, including remote management (e.g., screen share/assist) and the collection of analytics and data from frontline endpoints. This is often where UEM vendor choice leads to a multivendor/product strategy if certain specialty device management use cases are required, with vastly different needs for "regular" employee device management functionality.
- **Adjacencies and tie-ins to a strong portfolio of complementary IT/system infrastructure software products should be sought.** Solutions such as identity, cloud access security brokers (CASBs), IT service management (ITSM), security information and event management, network security, and line-of-business/vertical-specific application platforms are all important for UEM vendor consideration. Since UEM software does not operate in a vacuum, it is critical that vendors go to market either with complementary IT software product portfolios or strong integrations and partnerships with key industry players.
- **The aim should be to manage the unmanaged.** Look for UEMs with capabilities for managing endpoint apps, access control, and security/compliance posture without full enrollment. Known as "MAM only" features, it is more critical than ever for UEMs to be able to manage and secure personal BYODs across all form factors — PCs/laptops, phones, tablets, wearables, and IoT devices. IT teams must deploy UEM tools that can address granular policy enforcement, security, and control over apps and data accessed by these devices as corporate-owned devices.

## 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.

### Microsoft

Microsoft is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software.

At the heart of its extensive product suite is Microsoft Intune, a cornerstone of the company's unified endpoint management offerings. Intune exemplifies Microsoft's commitment to providing seamless, secure, and efficient management solutions for devices across the enterprise landscape. By integrating advanced analytics, AI, and automation into Intune, Microsoft is not just simplifying IT operations but fundamentally transforming how devices are managed, securing a leading position in the UEM market.

The Microsoft Intune product is part of a broader suite of management, security, and system infrastructure software products tied to the Microsoft 365 technology stack and licensing scheme. After a few iterations of branding and positioning, Microsoft has established Intune as its prime UEM offering and cloud-based endpoint management tool. While the vendor still supports and develops the Microsoft Configuration Manager (formerly System Center Configuration Manager [SCCM]) product for on-premises PC management, it is seeing rapid adoption of cloud-based PC, as well as mobile and macOS device management, with Configuration Manager used as a tool to migrate workloads to cloud management.

Microsoft's strategy revolves around leveraging innovation, simplifying management through cloud-based solutions, and reducing complexity and cost. Microsoft continues to evolve Intune by integrating AI and automation to enhance endpoint security and management capabilities. In particular, device error remediation, end-user experience monitoring, and threat detection and evaluation are primary AI/automation use cases for Intune and Microsoft overall.

While Microsoft is known primarily for Windows PC management, the vendor has made significant strides in managing Apple Mac devices over the past 18 months, with enhanced support for macOS, including secure enrollment and advanced configuration options. Intune's capabilities for managing frontline and ruggedized devices have also grown, including support for Android Open Source Project (an open version of Android used in many IoT endpoints and wearables, such as Meta's Quest headsets). Support for Zebra devices was also expanded with the integration of LifeGuard for over-the-air updates for the ruggedized endpoints. Windows management is the core strength of Intune. From an SMB perspective, Intune offers a strong solution by integrating with Microsoft 365 and streamlined management capabilities helpful for smaller IT teams or SMB-focused managed service providers.

## Strengths

Intune's integration with other Microsoft products enhances security and productivity and can offer a comprehensive and cohesive management and security solution. Intune is included in Microsoft 365 E3, E5, and Frontline licensing schemes, alongside dozens of Microsoft's other bedrock enterprise applications and tools (Windows, Office, Exchange, OneDrive, Teams, etc.).

Microsoft's Intune Suite— a package of management, remote help, endpoint privilege management, cloud-based private key infrastructure (PKI) remote access, and other key functions — offers strong packaging options for midsize companies as well as some enterprises.

Microsoft Intune supports a wide array of devices, including iOS, Android, Windows, Linux, and macOS, making it a versatile tool for organizations with diverse device ecosystems. Intune supports conditional access, advanced threat protection, and strong compliance policies in providing robust security measures to protect corporate data across all managed devices.

## Challenges

While Microsoft offers strong endpoint protection and identity tools (Microsoft Defender, Entra, etc.), the vendor has fewer official partnerships and integrations with third-party products in these areas as compared with other leading vendors in this document.

While Intune's reach has expanded into specialized areas of UEM, including Apple management and ruggedized/frontline device management, Microsoft faces strong competition from vendors that offer more specialized or customizable UEM solutions for these use cases — many of which are often deployed alongside Intune among enterprises.

### *Consider Microsoft When*

Microsoft Intune offers a comprehensive set of management capabilities, deep integration with a trusted ecosystem, and a strong focus on security. Enterprises and SMBs should consider the platform if they have Windows-first, heterogeneous PC environments with mobile devices function in multiple use cases.

## 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 market. Software products in this submarket combine, into a single software platform, the management and provisioning functions for most common end-user computing operating systems and device types (i.e., Windows, macOS, iOS, Android, and ChromeOS). By definition, UEM products must be able to manage both mobile (smartphone/tablet) and PC (desktop/laptop) endpoint device form factors (although support for multiple OSs in each device category is not a requirement). This excludes legacy platforms such as PC life-cycle management (PCLM), PC imaging solutions, mobile-only MDM platforms, and industrial IoT endpoint management platforms.

## LEARN MORE

### Related Research

- *Five Trends to Watch in Endpoint Device Management in 2024* (IDC #US51763224, January 2024)
- *The Role of Client Endpoint Management Tools in Digital Employee Experience Monitoring* (IDC #US46460821, December 2023)
- *Worldwide Unified Endpoint Management Software Forecast, 2023-2027* (IDC #US47945922, July 2023)
- *IDC MaturityScape: Apple Device Management in the Enterprise 1.0* (IDC #US50671623, May 2023)
- *What's Behind the Windows/Mac Device Management Gap in the Enterprise?* (IDC #US50688223, May 2023)

### Synopsis

This IDC study presents a vendor assessment of the unified endpoint management software market through the IDC MarketScape model.

"Employees in digital enterprises are most productive and effective at their jobs when their devices are familiar and usable, configured properly, and are provisioned with critical apps and software tools," says Phil Hochmuth, research VP, Endpoint Device Management and Enterprise Mobility at IDC. "UEM software plays a critical role in employee enablement by ensuring all device types — desktops to smartphones, wearables, and IoT endpoints — are prepared and secured for any and all required 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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

## Global Headquarters

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

---