IDC MarketScape

IDC MarketScape: Worldwide Unified Endpoint Management Software 2025–2026 Vendor Assessment

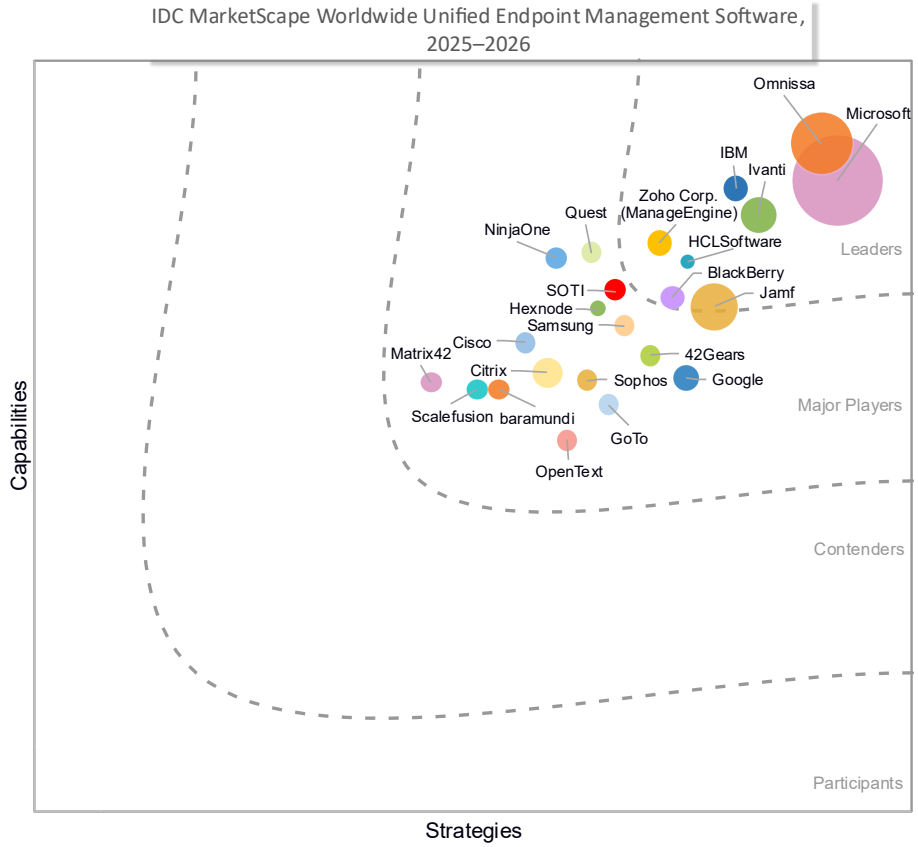
Phil Hochmuth

THIS EXCERPT FEATURES MICROSOFT AS A LEADER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Unified Endpoint Management Software Vendor Assessment



Source: IDC, 2025

December 2025, IDC #US53003125e

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

ABOUT THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Unified Endpoint Management Software 2025–2026 Vendor Assessment (Doc # US53003125).

IDC OPINION

The unified endpoint management (UEM) market continues to evolve as enterprises prioritize the consolidation of endpoint management tools and alignment with wider digital transformation and security initiatives. UEM platforms — originating from the merger of separate PC life-cycle management and enterprise mobility management (EMM) traditions — now serve a critical role in managing an increasingly complex array of devices, operating systems, user roles, and business objectives. According to recent enterprise surveys, most organizations run multiple UEM platforms, with consolidation among leading vendors advancing, yet the market remains characterized by a broad ecosystem of established and emerging providers delivering viable solutions.

A key industry dynamic involves balancing the ideal of a single unified platform with the practical needs for advanced use case and function-specific management. Enterprises report that full convergence is often stymied by the diversity of use cases: frontline workers, field staff, knowledge employees, and device fleets operating on a mix of Windows, Mac, iOS, Android, Chromebooks, and specialized IoT or single-purpose devices. As a result, many organizations adopt multivendor UEM deployments, choosing specific tools based on best-fit features for distinct operational or regulatory demands.

The convergence trend is further shaped by a growing emphasis on security, compliance, digital employee experience (DEX), and integration. Enterprises increasingly demand interoperability of UEM tools with adjacent system infrastructure — including identity and access management (IAM), endpoint security, security information and event management (SIEM), IT asset management, and business applications. Modern UEM must not only provide deep policy and provisioning control but also deliver actionable analytics, support for granular conditional access, and have the ability to measure and optimize user productivity, device health, and software performance over time.

At the same time, device and management diversity is accelerating. Businesses face rising expectations for UEMs to manage wearables (such as AR/VR headsets and digital signage), IoT devices, and traditional PCs and mobile devices within one framework. Support for new OS management methods — such as agentless mobile device

management (MDM) protocols and extensive declarative management — complements traditional agent-based approaches, offering greater flexibility for hybrid and remote work scenarios.

Ultimately, the UEM market is defined by a tension between unification and specialization. The leading platforms distinguish themselves by breadth of device support, portfolio depth, analytics and automation, and robust partner ecosystems. Meanwhile, IT decision-makers recognize that ongoing adaptability, strong security postures, comprehensive reporting, and seamless integrations are essential to capitalizing on the true value of enterprise UEM.

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 calendar year 2024. Revenue was estimated in February 2025 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:

- Note that when evaluating UEM platforms, prioritize those that offer comprehensive device coverage across Windows, macOS, iOS, Android, Chrome OS, wearables, and IoT endpoints. Achieving support for all major platforms from a single solution can greatly minimize management silos, facilitate consolidated policy enforcement, and simplify user provisioning.
- Choose UEM products that enable true single-pane-of-glass management, which means IT administrators can monitor, configure, secure, and report on all endpoints from one unified interface. This centralized approach not only saves valuable IT staff time but also increases visibility, reduces risks of human error, and drives operational efficiency across the board.
- Assess each solution's degree of prebuilt integration with core IT management and security infrastructure — including identity providers, IT service management (ITSM), SIEM, endpoint detection and response (EDR), and asset management platforms. Tight integration is essential for automating workflows,

linking compliance reporting, and ensuring that security incidents or IT support tickets are contextually aware of device state and user identity.

- Place significant weight on the UEM vendor's ability to deliver context-aware conditional access policies. These should not only govern access based on user role or group but also dynamically take into account device risk posture, geographic location, time of access, network quality, and OS or patch level, enabling more adaptive security management.
- Seek platforms that provide effective digital employee experience analytics, capturing data on device health, application usage patterns, and end-user satisfaction metrics. Enterprises benefit when IT can proactively identify and remediate sources of end-user friction, such as frequent system crashes, poor connectivity, or sub-optimal software experiences.
- Ensure the UEM supports a hybrid approach to device management, combining modern MDM-like protocols with traditional agent-based controls when necessary. This dual capability allows organizations to manage legacy devices and modern endpoints efficiently, reducing disruption as endpoints migrate to newer operating systems and deployment models.
- Consider strong remote support and troubleshooting capabilities indispensable, especially for supporting distributed, frontline, or remote employees. Look for embedded tools such as unattended remote control, chat, screen sharing, and automated device diagnostics, which enable faster resolution of issues without requiring physical device access.
- Ensure the system generates robust dashboards and drill-down reports covering device and app compliance, security vulnerabilities, OS and app patching status, and hardware life-cycle KPIs — comprehensive, customizable reporting is critical. Well-designed reporting features play an essential role in maintaining audit readiness and guiding investment in hardware refresh and support resources.
- Note that automation must be a core consideration, encompassing both workflow automation for tasks like onboarding/offboarding, patch deployment, and policy enforcement and auto-remediation of common issues. Automation reduces manual workloads and ensures policy consistency, especially in organizations scaling up device fleets or adopting increasingly complex compliance regimes.
- Examine the vendor's road map for incorporating next-generation features, such as AI-driven anomaly detection, predictive analytics for hardware failure, or zero trust remote security posture checks. Selecting a vendor with clearly articulated plans for innovation helps future-proof your investment, ensuring your endpoint management strategy can adapt to rapid changes in workforce tools and threat landscapes.

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 2025–2026 IDC MarketScape for worldwide unified endpoint management software.

Microsoft, headquartered in Redmond, Washington, and founded in 1975, offers its unified endpoint management solution under the product family "Microsoft Intune." Intune is designed to deliver a single pane of glass for comprehensive device management, unifying the configuration, security, and life-cycle management of corporate and personal devices across Windows, macOS, iOS/iPadOS, Android, and specialized endpoints. Key features include policy-based provisioning, configuration and compliance management, advanced app life-cycle controls, remote support, robust analytics, device health monitoring, and advanced automation with generative AI through Copilot for Intune. Intune leverages deep integration with additional Microsoft services, including Microsoft 365, Defender for Endpoint, Entra ID (formerly Azure Active Directory), and Microsoft Security Copilot for advanced security and identity management workflows. The platform also enables powerful third-party integrations via Microsoft Graph API, application catalogs, IT service management connectors (such as ServiceNow), and SIEM/SOAR platforms to support broad enterprise automation and incident response. Partnerships with prominent managed service providers and ecosystem solution vendors enhance multitenant management and enable a wide variety of vertical and geographic customer needs. Microsoft maintains a strong commitment to the channel, with ongoing initiatives to enable partners, encourage managed SP-centric workflows, and invest in self-service, automation, and customer adoption at scale.

Strengths

- Advanced integration with Microsoft cloud identity, security, and productivity platforms, driving low-friction, highly automated management for organizations that standardize on Microsoft 365 ecosystems
- Comprehensive support for modern workplace security, zero trust access, and device compliance through integrated tools such as Defender for Endpoint, Endpoint Privilege Management, and advanced role-based access controls

- Intuitive automation and analytics, including Copilot-powered AI assistance, device and user experience monitoring, and guided remediation workflows that enhance IT operational efficiency
- Extensive partner and ISV ecosystem that enables organizations to leverage Intune as a platform for layered security, automation, device life-cycle orchestration, and value-added industry-specific solutions

Challenges

- Customers heavily invested in non-Microsoft platforms and environments may encounter integration limitations or operational overhead beyond core Microsoft OS and service support.
- Organizations with legacy or highly specialized device fleets (non-Windows or non-standard devices) may require third-party products or additional investments for equivalent management depth.
- Advanced features for certain platforms (notably macOS and iOS) may lag in parity or require adaptation from legacy management approaches, necessitating change management for existing teams.
- Full realization of AI-driven management and Copilot assistance is still evolving, with some features in preview or early stages of enterprise adoption.

Consider Microsoft When

Organizations seeking maximum value from Microsoft 365 licensing, unified device and security policy management, and deep integration with Microsoft's cloud and security ecosystem should prioritize Microsoft Intune when selecting a UEM platform. Buyers looking to modernize endpoint management, leverage AI-driven workflows, and reduce complexity through single-platform management should include Microsoft's UEM offering in competitive evaluations.

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 Chrome OS). 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

- *Market Analysis Perspective: Worldwide Client Endpoint Management, 2025* (IDC #US53787225, October 2025)
- *IDC TechBrief: Digital Employee Experience* (IDC #US53638125, July 2025)

- *Worldwide Client Endpoint Management Software Market Shares, 2024: Preparing for a More Automated World* (IDC #US53140725, June 2025)
- *Worldwide Unified Endpoint Management Software Market Shares, 2024: A UEM for Every Use Case* (IDC #US53140625, June 2025)
- *Worldwide Unified Endpoint Management Software Forecast, 2025–2029* (IDC #US53140525, June 2025)
- *Worldwide Client Endpoint Management Software Forecast, 2025–2029* (IDC #US53140425, June 2025)
- *Five Trends to Watch in Endpoint Device Management in 2025* (IDC #US53081125, January 2025)

Synopsis

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

"Digital transformation of businesses starts with endpoint devices — from laptops and workstations to smartphones and tablets to specialized and connected equipment," says Phil Hochmuth, research VP, Endpoint Device Management and Enterprise Mobility, IDC. "As productivity, revenue, and other critical operations rely more on device availability and security, IT teams must keep pace with converged, AI-enhanced endpoint management software platforms."

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

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC at customerservice@idc.com for information on additional copies, web rights, or applying the price of this document toward the purchase of an IDC service.

Copyright 2025 IDC. Reproduction is forbidden unless authorized. All rights reserved.