IDC MarketScape

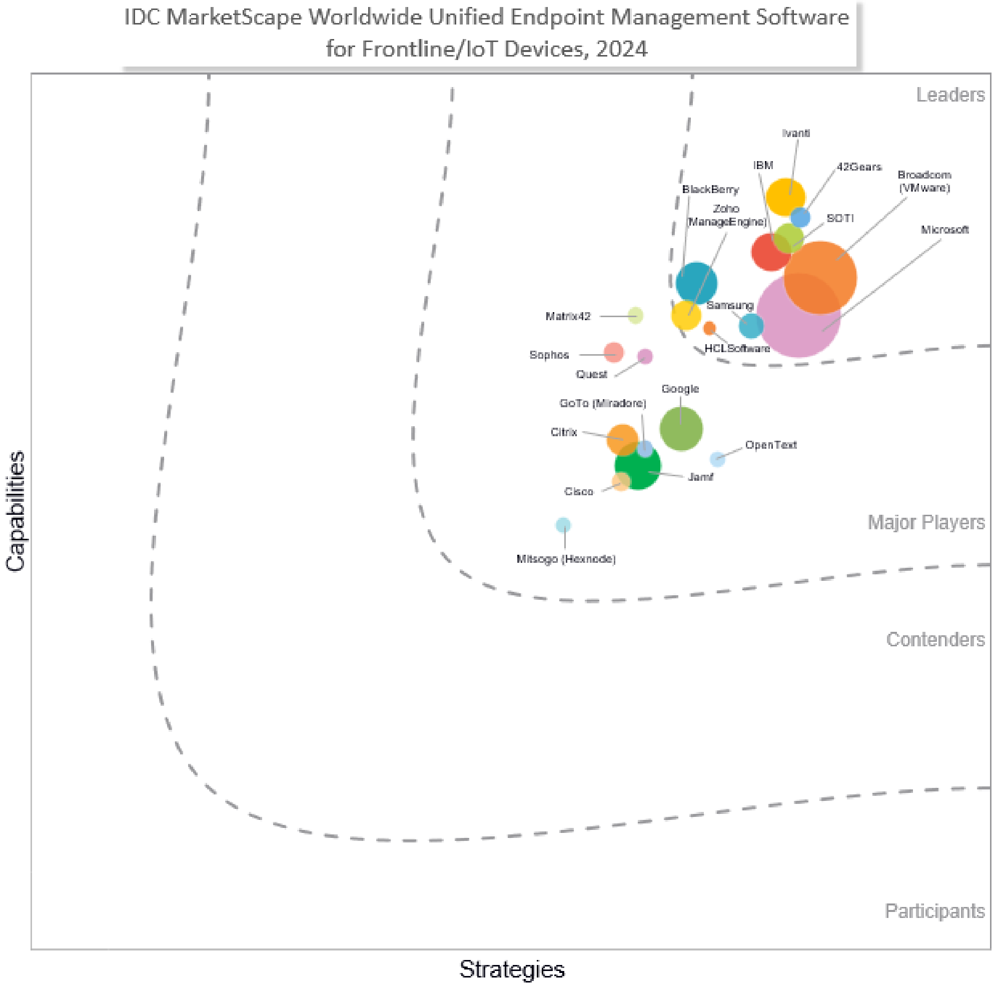
IDC MarketScape: Worldwide Unified Endpoint Management Software for Frontline/IoT Devices 2024 Vendor Assessment

Phil Hochmuth

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Unified Endpoint Management Software for Frontline/IoT Devices Vendor Assessment



Source: IDC, 2024

April 2024, IDC #US51779324

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

IDC OPINION

Enterprise digital transformation often begins/ends with endpoint devices. Frontline workers' roles are evolving and are being affected by digital change; analog tools and old ways of operating (e.g., paper-based processes) are digitizing, resulting in the introduction of a new devices, and new workflows are created around these endpoints. Myriad examples of this exist across industries: tablets replacing clipboards or logbooks in hospital rooms or long-haul delivery trucks; big-box retail workers using in-store smartphones for merchandise inventorying or product look-ups; and car mechanics or delivery persons snapping smartphone pictures of a repair job or package delivery, with the media automatically sent to customers. At the same time, specialty endpoint devices in various industries have also evolved, often moving to standardized smartphone/tablet devices and operating systems (OSs) (e.g., Android).

All these specialized device use scenarios require a different approach to device management compared with standard unified endpoint management/mobile device management (UEM/MDM) use cases. Frontline and IoT devices are more often likely to be locked down in terms of what they can be used for or even the locations they're allowed to be used. Close monitoring of activity is a requirement as well as gathering critical telemetry off the devices for management and operational purposes (e.g., measuring device battery life, pinpointing device location in facility/plant). According to IDC's 2023 *Enterprise Endpoint Device Survey,* more than 70% of organizations use multiple UEM platforms in their environment; often, a UEM tool for ruggedized/IoT device management is a common second platform. As more varying endpoint types become connected in offices (wearables such as watches and headsets as well as connected conference room gear, digital signage, and building controls), UEM tools will come into play as a potential management platform.

Some vendors in the market aim to specialize their UEM tools for ruggedized/IoT endpoints. Other vendors' offerings are presented as capable of incorporating all of these device management scenarios into a single UEM product. For success in managing ruggedized/IoT and special-purpose endpoint devices, vendor products and strategies should focus on the following areas:

- **Strong endpoint controls and lockdown capabilities:** UEM tools must be able to apply restrictions on endpoints to only allow usage of a single app or a set of specific apps and services required for a deployed use case or workflow involving the device.
- **Multiuser support and enablement:** Shift worker scenarios, where a frontline device is used by multiple employees throughout the workday, require multiple log ins/log outs on a device. UEM tools must be able to support this function while helping devices tie to back-end identity and business application platforms.
- **Granular device management telemetry and analytics:** Enterprises require close monitoring and tracking of frontline/IoT device usage for a number of reasons. Tracking device performance (to anticipate battery drain, downtime, or troubleshooting) and physical location (ensuring the device is being used how and where it should be) are among the key telemetry data businesses with frontline/IoT endpoint operations must track and analyze.
- **Strong relationships and partnerships with device OEM and industry software vendors:** Specialty device makers (e.g., Zebra, Dialogics, Panasonic, Honeywell, Kyocera, Samsung) have close relationships with enterprises and organizations using these frontline endpoints. UEM vendors must have partnerships and relationships with these providers, as well as support for vendors' proprietary or specialty technology requirements.

- **A focus on Android:** The Android operating system is the most widely used endpoint technology in most frontline/IoT endpoint device deployments. UEM tools must be able to granularly manage Android in these use cases, as well as extend management and control functions to noncommercial/standard versions of the open source software platform (e.g., Android Open Source Project [AOSP]).
- **Flexibility and openness to manage nonstandard endpoint operating systems and form factors:** Enterprise workspaces are expanding beyond traditional device operating systems, including wearable technology, conference room/meeting space devices, and workspace IoT endpoints. watchOS, Wear OS, Tizen, Linux, Raspberry Pi, QNX, and other embedded real-time operating systems must be manageable by UEM tools.

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 2023. Revenue was estimated in February 2024 and may differ from forthcoming market share documents.

ADVICE FOR TECHNOLOGY BUYERS

- **The workspace and device requirements of frontline workers, multiuser endpoints, field workers, and deskless workers should 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 of ruggedized endpoints, and field workers should be as extensible as standard UEM device support, including remote management (e.g., screenshare/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.
- **Multi-UEM is not an oxymoron; there may not be one UEM to rule them all.** According to IDC's 2023 *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. Frontline device management, as well as IoT management, is a scenario that fits this model well. It is not uncommon for management of such devices to fall outside of a central IT or endpoint management team, where line-of-business teams or operational technology (OT) teams control the use of specialty devices.
- **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. Frontline workers' digital experience is critical to measure for the purposes of staff retention, productivity monitoring, compliance, and optimization of workflows and operations.

- **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 of or health of the device being used (from the standpoint of a jailbroken/rooted device or an operating system that is out of date). Frontline devices must be seamlessly secure when deployed in the correct location, facility, or use case. UEM tools must be able to detect deviations from these normal operational environments and apply policies and security controls accordingly.

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.

42Gears

42Gears is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Founded in 2009, 42Gears, based in Bangalore, India, has operations worldwide and now has over 300 employees. The company provides a wide range of products, from basic MDM solutions in its product to a full-featured UEM solution. Its SureMDM product can manage a wide range of devices, including Android, Apple, and Windows endpoints. One of its specialized areas is in the management of ruggedized and IoT devices. By aligning with ruggedized device OEMs and integrating with platforms like Google's Android Enterprise and Zebra Technologies, 42Gears has expanded its reach and capability to manage a broad spectrum of devices efficiently.

From a mobile device perspective, 42Gears supports Android Enterprise Recommended, aligning with the program's standards of security and management. SureMDM also provides integration with Apple Business Manager, enabling simplified device enrollment and configuration for macOS/iOS/iPadOS endpoints. For Windows, 42Gears includes patch management and administrative template management. 42Gears' flexible pricing and scalability make the company an attractive option for small and medium-sized businesses (SMBs) as well.

Strengths

Device management breadth is a strength of SureMDM. 42Gears excels in offering extensive support across various device types, including mobile, desktop, and IoT devices (including Linux-based devices) and AOSP endpoints.

Security, especially Android security, is a strong focus of 42Gears UEM tools. With integrations for mobile threat management, dedicated VPN, and identity management solutions, 42Gears ensures a secure environment for enterprise devices against evolving cyberthreats.

User support, especially for frontline and ruggedized device use cases, is a strong suit for 42Gears; the platform has integrated remote assist tools, including this capability for remotely viewing and taking over the screen of Windows, iOS, and Android mobile devices, which is a critical requirement for frontline mobile deployment use cases.

Challenges

Like other smaller or specialized players in the UEM market, 42Gears faces competition and challenges as others look to consolidate more endpoint management. The UEM market is highly competitive, and standing out requires continuous innovation and the ability to address unique customer needs efficiently.

Consider 42Gears When

Consider 42Gears SureMDM for its comprehensive device support, advanced security features, and user-friendly administration interface. Its strategic focus on partnerships and certifications is another factor to consider for firms deploying UEM alongside other integrated systems and platforms (e.g., line-of-business apps, VPN/connectivity platforms, workforce management solutions). Companies looking to streamline their device management processes and enhance operational efficiency should also consider 42Gears specifically for frontline and rugged device deployment scenarios.

BlackBerry

BlackBerry is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

BlackBerry, based in Waterloo, Ontario, Canada, specializes in endpoint device management and endpoint security software. BlackBerry's UEM solution is a key component of its larger cybersecurity portfolio, including its security products based on Cylance technology, as well as data, voice communications, and mobile device OS security tools. Via the Cylance technology, BlackBerry integrates AI and machine learning throughout its product portfolio, including BlackBerry UEM. The vendor has released its own integrated mobile threat defense (MTD) product and offers a range of secure digital file sharing, mobile application wrapping, and secure mobile messaging tools. BlackBerry supports both cloud and on-premises deployments, allowing businesses to meet their operational and security needs. This also suits security-conscious firms looking for hybrid on-premises UEM deployments for security or data protection/sovereignty purposes.

Continuous investment in user experience (UX) improvements across iOS and Android platforms ensures a user-friendly interface, promoting user adoption and satisfaction. BlackBerry UEM has also added enhanced support for iOS devices, including recent UX improvements and a rich integration between BlackBerry Work and the Apple Watch. BlackBerry's emphasis on security and productivity also balances well with Windows environments, particularly through integration with Microsoft Intune. This continual enhancement of integrations to meet evolving enterprise needs is critical.

Strengths

BlackBerry UEM meets a wide range of compliance and security regulatory requirements, including FIPS, FedRAMP, and Common Criteria EAL 4+, making it a UEM platform of choice for firms in highly regulated industries such as banking and government. BlackBerry UEM provides strong data-at-rest and data-in-transit security without relying on the host OS for security measures. The platform also has strong app wrapping and data isolation via containerization for mobile devices.

BlackBerry UEM supports a wide range of devices, including smartphones, tablets, wearables, and IoT devices. The vendor's experience in embedded computing (e.g., its QNX real-time OS) and critical event management platform (AtHoc) also tie into the vendor's overall value in supporting frontline and critical operations environments with device management and security.

Planned initiatives for frontline/ruggedized device management for integration with Zebra devices indicate BlackBerry's focus on support for frontline workers.

The flexibility of BlackBerry UEM's deployment models and its security features are a draw for SMB customers, which the company is refocusing to support and address. The vendor's large roster of cellular/mobile operator partners is another strength in addressing SMB needs.

Challenges

In its large enterprise customer base, BlackBerry needs to maintain and grow its market share to stand up against broader IT operations, security, and productivity platforms found in the market. Navigating this competitive landscape will require ongoing innovation and differentiation to maintain and grow market share.

Longtime CEO John Chen's retirement and John Giamatteo's appointment as CEO in 4Q23 marked a significant leadership shift at BlackBerry. The company will now run IoT as a separate business unit to Cybersecurity, with each unit gaining autonomy over respective business strategies. Under the new CEO, the focus is on how the two main business units (IoT and Cybersecurity) will both collaborate and operate independently, to jointly advance the company's momentum. With new leadership, how this strategy evolves remains to be seen.

Consider BlackBerry When

BlackBerry UEM stands out for its robust security features, comprehensive device support, and user-centric improvements. For companies prioritizing security, compliance, and a diverse device ecosystem, BlackBerry UEM offers a strong solution that aligns with the needs of modern enterprises and their mobile workforce.

Broadcom (VMware)

Broadcom (VMware) is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Broadcom's VMware flagship UEM product is its Workspace ONE platform. The platform is designed to address the complexities and challenges of hybrid work environments, as well as specialty device management use cases, offering solutions for diverse endpoint types through a single management interface.

Workspace ONE integrates device management across a broad range of operating systems (Windows, GMS/AOSP Android, macOS, iOS/iPadOS, ChromeOS, Linux, and others). It also combines management with access control, application management, security/compliance, and endpoint analytics. Workspace ONE has strong capabilities in managing macOS and iOS, by integrating with Apple Business Manager for streamlined enrollment and management processes as well as for supporting advanced features such as platform single sign-on for Mac devices and declarative device management for iOS and macOS endpoints. Frontline and ruggedized device management is another strongpoint for Workspace ONE, delivering management, proprietary application Launcher, and remote support capabilities for AOSP-based, Zebra, and other specialty endpoints for dedicated use cases. Workspace ONE has also evolved to be a challenger to Microsoft in terms of Windows device management functionality, covering a range of Windows 10/11 endpoint scenarios, including multiuser use cases.

Add-ons to Workspace ONE in which the company has seen strong growth include its Freestyle Orchestrator module, which allows IT professionals to create complex workflows and automations, and Workspace ONE Intelligence, a Digital Employee Experience solution, which can gather telemetry from device, app, and user behavior and provide visibility and analysis into end-user device issues. The vendor has also demonstrated road map features for integrating AI and natural language processing across the platform.

Strengths

Workspace ONE has one of the most complete combined management feature sets across Windows and Apple Mac PC management, going deep in terms of feature support, patching, enrollment, and life-cycle management for each respective platform.

Workspace ONE has an array of supporting apps and tools — such as Workspace ONE Intelligent Hub — as well as productivity apps (e.g., Workspace ONE Boxer), which provides enhanced, organized, and secured access to corporate apps, data, and resources.

The adjacent Horizon virtual desktop and app virtualization tools offered by VMware/Broadcom's End-User Computing (EUC) group tie together well with the vendor's UEM solutions from a portfolio and integration standpoint.

Challenges

Shortly after the finalization of the VMware acquisition by Broadcom Inc. in November 2023, Broadcom announced in February 2024 the plan to divest the End-User Computing division from VMware. The divestiture aims to create a standalone entity with financial backing from investment firm KKR. This is a lot of change for VMware/Broadcom in six months. The software maker must assure customers that vendor/channel relationships, road maps, and operations will go on as expected as the EUC division separates from VMware/Broadcom.

While Workspace ONE offers deep, advanced management and security for large, multi-OS device deployments, its solutions can be complex and a challenge to implement for smaller customers. The vendor offers Workspace ONE Essentials offerings as an alternative solution for SMBs.

While Workspace ONE is positioned well to handle large enterprise needs for unified Windows and Mac management, many large firms with management needs for both platforms opt for splitting support of these use cases across multiple UEM providers with specially focused features for each respective endpoint type.

Consider Broadcom (VMware) When

Organizations seeking a comprehensive UEM solution with advanced orchestration, analytics, and AI features should consider Workspace ONE. The platform is among the most complete UEM products on the market, capable of handling nearly every endpoint device management scenario, use case, and market requirement.

Cisco

Cisco is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Cisco is a prominent global networking and IT security product vendor. The company offers a UEM solution focused on converged, integrated network infrastructure targeted at enterprises as well as SMBs. Meraki Systems Manager is focused on simplified IT management and enhancing security in an increasingly complex and threat-prone digital landscape.

Meraki Systems Manager covers a wide range of devices, including iOS/iPadOS, macOS, Android, Windows, and ChromeOS. Simplification is a key strategy for Cisco's UEM product, allowing businesses to manage diverse device ecosystems more efficiently in line with the increasing security threats to IT environments. Cisco's integration of the company's security products with the Meraki Systems Manager offers a robust and comprehensive approach to endpoint security. This includes its identity platform (Cisco Identity Services Engine [ISE]); its Duo two-factor/mobile security offering; Cisco Umbrella, a DNS-based cloud security and data protection service; and Cisco's wide range of Meraki network security products (firewalls, IPS, VPN concentrators, and secure Wi-Fi technology).

Strengths

Cisco emphasizes security interoperability and a unified approach with Meraki Systems Manager and other solutions from the Cisco security portfolio, including Duo and Umbrella, as part of a zero trust endpoint management solution.

Cisco provides a unified, single dashboard for managing all endpoints, greatly simplifying IT operations. This converged interface is a significant strength, making it easier for IT teams to manage and monitor their device ecosystems. The Meraki dashboard provides configuration, security tools, and full management capabilities for the entire network, allowing IT teams to monitor and control a large network of devices and endpoints.

Challenges

Much of the value of the Meraki Systems Manager comes from the integration with other Cisco networking and security solutions. This makes the technology a strong solution for environments where Cisco infrastructure is present. Meraki Systems Manager loses some of these advantages when managing devices of remote workers in home network environments or for mobile workers connected to noncorporate network infrastructure or cellular networks.

While Cisco provides integrations with a wide range of systems, integrating the Meraki Systems Manager with existing legacy systems can be challenging for some organizations. Unfortunately, Cisco has few third-party patch management, SIEM, and endpoint security product integrations.

Consider Cisco When

Meraki Systems Manager has significant strengths like comprehensive security integration and support for a wide range of devices. Organizations with small IT teams responsible for a large amount of endpoints, as well as Cisco-centric infrastructure customers, will benefit from Cisco's strategy of simplification and security focus and providing scalable cloud-based UEM solution.

Citrix

Citrix is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Citrix's strategy revolves around leveraging cloud technology to enhance endpoint management. The company has positioned CEM as a cloud-first solution, enabling seamless migration from on-premises to cloud environments. This approach not only simplifies IT operations but also ensures that businesses can easily adapt to the evolving demands of mobile productivity. Citrix's integration with Citrix Workspace enhances this offering by providing a unified platform that facilitates secure access to apps and data, effectively catering to the needs of modern enterprises.

CEM provides strong support for iOS devices, ensuring comprehensive management capabilities, as well as Frontline devices, and addresses the needs of diverse industries. Windows Device Management has always been a strength of Citrix from its history in working with Microsoft OS platforms. CEM provides deep integration with Windows 10 for modern management capabilities.

Strengths

- **Comprehensive device support:** Citrix Endpoint Management stands out for its broad device support, including iOS, Android, Windows, Chrome OS, and even rugged devices. This versatility ensures that enterprises can manage a diverse range of devices under a single umbrella, simplifying IT operations.
- **Cloud-first approach:** The cloud-based nature of CEM allows for scalability, flexibility, and enhanced security features. This approach aligns with the digital transformation goals of many organizations, making it an attractive choice for businesses looking to modernize their endpoint management.
- **Integration with Citrix Workspace:** CEM's integration with Citrix Workspace offers a cohesive experience, facilitating not just device management but also secure access to applications and data. This integration is a significant advantage, providing users with a seamless experience across devices and improving overall productivity.

Challenges

UEM is less of a priority for Citrix as the vendor has shifted its product development and marketing focus almost entirely toward its virtual desktop and application streaming technologies. Citrix products are now developed and sold by the Cloud Software Group, a merged software entity of Citrix and TIBCO, owned by Vista Equity Partners. While still offering and supporting its UEM product, Cloud Software Group has made the strategic decision to focus product development, marketing, and sales efforts around its virtual desktop infrastructure (VDI) and desktop as a service (DaaS) as well as its Citrix Workspace app. Citrix Endpoint Management is positioned as a supporting tool for the vendor's App Security portfolio, which includes its Remote Browser Isolation product and Secure Private Access and Analytics for Security tools.

Retaining its existing UEM customer base will be a challenge for Citrix. In customer reference interviews and survey data gathered for this document, multiple organizations with Citrix Endpoint Manager in their environment said they were actively looking to migrate to another platform for their primary UEM technology.

Consider Citrix When

Citrix Endpoint Management is still a strong complementary UEM product for integration with Citrix Workspace and other Citrix client-focused virtualization technologies.

Google

Google is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Google Endpoint Management is a component of the Google Workspace suite and targets devices running Google Workspace apps and services. The platform supports Windows, macOS, Android, iOS, and ChromeOS and can provide standard management functions (OS configuration and updating, app distribution, policy deployment/enforcement, etc.) as well as deeper, more sophisticated actions, such as enforcing, conditional access rules, and other advanced features. For Windows device management, Google Credential Provider for Windows (GCPW) service works with Windows 10/11 endpoints and allows Google Workspace accounts to be used as Windows log-ins, providing single sign-on features for Chrome and Google Workspace apps, as well as data management and device inventorying. For Macs, Google Endpoint Management can provide strong management of Google Workspace data and access controls for Mac users. Android and iOS management includes security certificate management for managed mobile devices, as well as MDM configuration, app distribution, data security, and device inventorying for enrolled smartphones/tablets. The platform also has capabilities to gather data and telemetry information from Linux endpoints and some smart home devices that can access Google Workspace data and services.

Strengths

Google's BeyondCorp data and identity-based security approach and principles are recognized widely as the future of security for cloud-centric enterprises and companies. Google Endpoint Management integrates these concepts of identity-based access controls and security policies tied to data and apps, as opposed to physical devices or their location or network attachment.

Google Endpoint Manager has strong security and management functions around Workspace apps, including cross-platform mobile/cloud apps management. It has strong data protection capabilities for securing sensitive data accessed and used by Google Workspace apps.

Challenges

Google Endpoint Management is a strong solution for managing devices using the overall Google Workspace enterprise app suite and security services. However, outside of this scenario, Google's UEM capabilities lag behind other vendors in terms of depth of features supported and the breadth of devices that can be managed by the platform.

Google Endpoint Manager has fewer capabilities around managing macOS devices compared with Android, iOS, and Windows (e.g., no remote data wipe for Macs, more limited account management on Mac endpoints).

Consider Google When

Organizations standardized on Google Workspace productivity apps should consider Google Endpoint Management for device management. Organizations with large numbers of Android devices, as well as SMBs adopting Google Workspace, Android, and/or ChromeOS at scale, should also consider Google as a UEM technology partner.

GoTo (Miradore)

GoTo (Miradore) is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Miradore, the Finnish UEM cloud software provider, was acquired by the United States–based GoTo Technologies USA, a maker of remote support, monitoring, management, and collaboration software. (Products include GoToMyPC, GoTo Resolve, LogMeIn Rescue, and GoTo Webinar.) Miradore operates as an independent subsidiary of GoTo, offering its cloud-based UEM product; focusing on providing a unified solution for managing a diverse array of devices, including iOS, Android, Windows, and Mac, and ruggedized devices; and catering to the specific needs of small and medium-sized businesses.

Miradore's strategy focuses on the integration of the company's UEM product into the broader IT management portfolio offered by GoTo, following the acquisition of Miradore by GoTo. This strategic move aims to leverage existing assets and brand equity in the SMB and managed SP markets to position Miradore as the primary UEM product. The company focuses on increasing its average revenue per user by introducing new product tiers that integrate GoTo's portfolio features, such as native remote access and IPaaS integrations with Okta and Entra ID (formerly Azure AD), enhancing the overall product offering. Miradore offers robust support for Apple devices, making it a strong contender for businesses heavily invested in the Apple ecosystem. The platform's ability to manage ruggedized devices is a significant advantage for industries that rely on these types of devices. The challenge lies in continuously adapting to the unique requirements and evolving technologies of these devices. With strong support for Windows devices, GoTo/Miradore appeals to organizations with a significant Windows device footprint. Miradore's ease of use and freemium model are particularly attractive to small and medium-sized businesses. To that end, the Miradore product is also targeted at managed service providers that provide bundled or value-added UEM services to SMBs, usually with other offerings such as security or other managed services.

Strengths

Miradore excels in providing a single platform that supports Android, Mac, iOS, and Windows devices, eliminating the need for multiple management systems and offering a unified user experience.

Miradore UEM is recognized for its user-friendly interface and ease of setup, which is particularly appealing to SMBs and managed SPs that may not have extensive IT resources.

Miradore offers a unique freemium model for MDM, which can be used for managing an unlimited number of devices. Miradore stands out in the market, providing basic MDM functionality at no cost, with flexible pricing for more advanced features. Businesses looking for greater functionality can upgrade to a paid version of the offering — a conversion model where the company has so far had success.

Challenges

Miradore competes primarily in a segment of the UEM market focused on SMBs, where low-cost device management solutions are commonly offered. Standing out and attracting new customers in such a crowded space is a constant challenge.

While Miradore covers the primary use cases for its target audience, it may lack the depth of granularity in feature functionality found in software that specializes in frontline/IoT device management.

Post-acquisition, GoTo must continue to integrate the Miradore technology with its complementary offerings while maintaining brand identity in a way that resonates with both existing and potential new customers. Keeping Miradore as a separate entity makes sense to a certain point; a stronger better-together approach integrating Miradore UEM with all GoTo products will likely be a more productive long-term strategy.

Consider GoTo (Miradore) When

Miradore Unified Endpoint Management stands out for its multiplatform support, user-friendly approach, and innovative freemium model, making it an appealing choice for businesses of all sizes. Organizations, especially SMBs, looking for a UEM solution that offers ease of use, flexibility, and strong multiplatform support should consider Miradore UEM.

HCLSoftware

HCLSoftware is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

HCL has grown its BigFix device management platform in the UEM market focusing on three core areas: comprehensive device management, advanced security features, and an integrated IT administrator/user experience. By integrating these elements, HCL aims to simplify endpoint management.

BigFix UEM offers extensive management capabilities across a wide range of devices, including support for Apple devices (mobile and PC), ruggedized devices for frontline use, Windows devices, and Android devices. The vendor, while enterprise in scale, also provides strong capabilities for use cases for small and medium-sized businesses; zero-touch provisioning, simple certificate deployment, VPN setup, and support for BYOD scenarios are among these features. Security and patch management are a particular focus for BigFix UEM, with features designed to protect against evolving threats. The platform offers unique security capabilities such as zero trust security models, certificate management enhancements, and integration with security APIs. HCL focuses on delivering enhanced user experiences through features like self-service apps, allowing employees to resolve common issues autonomously. This not only improves user satisfaction but also reduces the burden on IT staff, making BigFix UEM an attractive option for organizations looking to improve efficiency and employee productivity. It has strong support for Apple devices, including zero-touch provisioning and enhanced security features. Capabilities like kiosk support for iOS and Android devices cater to the unique needs of frontline workers. The BigFix offering is scalable and modular, allowing it to grow with customers' businesses and device fleets.

Strengths

BigFix UEM's ability to manage a wide array of devices, including specialized ones like ruggedized and Apple devices, provides HCL with a competitive edge.

The platform's focus on advanced security features and compliance management appeals to organizations prioritizing cybersecurity and deep integration with Windows environments, including advanced features like offline domain join and certificate management. The vendor also has a broad set of Windows patch management (as well as third-party Windows app patching).

With features aimed at simplifying device management and enhancing user experiences, HCL helps organizations reduce IT overhead and improve productivity.

Challenges

While the vendor has gained a significant number of managed mobile devices since it first launched mobile OS support in BigFix (making the platform a true UEM), it has mostly grown its mobile devices under management among its existing BigFix customer base. It has been less successful winning net-new mobile management business as a standalone UEM offering.

The UEM market is highly competitive, so standing out requires continuous innovation and differentiation.

While SMBs can greatly benefit from the features and functionality of BigFix, for smaller organizations or those with limited IT resources, the complexity and implementing the full BigFix stack can be challenging.

Consider HCLSoftware When

Companies seeking a robust UEM solution that balances security with user-friendliness should consider HCL BigFix UEM as a key contender in their selection process, especially if granular OS and app patch management, integration with third-party IT platforms, and consolidated dashboards and console interfaces are a priority.

IBM

IBM is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

IBM's UEM product, MaaS360, is a cloud-based offering that is part of the vendor's large security portfolio. MaaS360 integrates device management, elements of endpoint security, and AI insights into a single platform, reducing the need for multiple solutions. MaaS360 is strong in both Apple Mac and Microsoft Windows device management, offering zero-touch deployment, extensive OS and app patching, and vulnerability management for both types of PC endpoints. It also supports a broad mobile device, application, and data management for iOS and Android devices – in standard mobility use cases as well as custom device management for specific use cases like healthcare. IBM has made significant investments in other frontline use cases as well, emphasizing security posture, user experience, and remote management capabilities for minimizing device downtime. The vendor's product-led ecommerce approach to marketing and selling MaaS360 is also helpful in targeting SMBs, and it provides smaller firms a simplified purchasing, deployment, and onboarding process for adopting MaaS360.

Strengths

MaaS360's comprehensive UEM functionality is a primary strength, in that the product covers a broad set of device types and OSs, but also goes deep into each technology in terms of management functionality, as well as control of apps, data, and settings.

IBM's product suite of security solutions integrates well with MaaS360, allowing customers with multiple IBM products to build a strong loop of management and security functionality across all endpoint types.

IBM's Watson AI platform is working to integrate with MaaS360, allowing customers to train AI models for generating recommendations, such as policy suggestions for new users and benchmarks for security standards. On the road map, AI will be able to predict device issues such as battery life, identify battery-draining applications, and suggesting actions to improve device longevity and user productivity.

Challenges

Beyond IBM security product tie-ins for MaaS360, IBM's product portfolio is limited in terms of IT infrastructure, system management, and other technologies directly impacting end-user computing and support.

While MaaS360 is backed by IBM's Watson AI platform with a strong road map around AI-enabled endpoint management, the vendor's current capabilities around using endpoint telemetry data to enhance user experience and IT device support are limited than offerings with more complete end-user support and IT service management infrastructure portfolios that are available in the market.

Consider IBM When

Companies should consider IBM MaaS360 for their UEM needs due to its robust platform that simplifies device management across various operating systems and its proactive approach to security and productivity enhancements. The platform is a viable option for either a complete endpoint management strategy via a single UEM or for deploying MaaS360 in specialized device management scenarios, such as ruggedized/frontline endpoints. SMBs will also benefit from the product's simplicity in purchasing, adoption, and rollout.

Ivanti

Ivanti is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Ivanti has evolved its approach to UEM, and its collective system infrastructure software portfolio overall, beyond a set of separate, externally acquired product lines into a more streamlined unified portfolio overall. Ivanti's strategy revolves around integrating advanced technologies such as AI and machine learning with a deep focus on improving the digital employee experience (DEX). The company emphasizes the convergence of UEM, IT security, and DEX, aiming to provide proactive, intelligent management and security solutions that do not compromise the user experience. By leveraging data and AI/ML, Ivanti aims to drive proactive endpoint management, reduce IT administration burdens, and mitigate risks through enhanced security views and remediation actions. This strategic integration positions Ivanti uniquely in the UEM market, enabling the company to address the evolving needs of businesses in managing and securing their endpoint landscapes.

Ivanti has strengthened its capabilities in managing Apple devices through partnerships and enhancements in declarative management, aligning closely with Apple's evolving management frameworks. From a Windows Device Management perspective, which is Ivanti's heritage, the product offers advanced patch management and security features and deep levels of policy control. Ivanti's ruggedized device management — in the past, a separate product offering — has evolved into a more singular UEM feature. The platform provides robust support for devices like Zebra. The vendor's underlying Neurons integration strategy also allows for broad automation scenarios across the device management, IT service management (via the Cherwell technology it acquired), and IT asset management platforms.

Strengths

Ivanti excels in managing a wide range of devices, offering robust support for everything from traditional PCs to mobile and IoT devices, ensuring comprehensive visibility and control over the endpoint environment.

The integration of AI and machine learning technologies enables Ivanti to offer intelligent and predictive endpoint management and security solutions, enhancing efficiency and proactive risk management.

Ivanti places a strong emphasis on DEX, providing tools and insights that enhance end-user satisfaction and productivity while ensuring devices are secure and compliant.

Challenges

"While Ivanti Neurons for UEM includes automation and AI for UEM, additional value proposition requires the broader adoption of Ivanti products beyond its UEM offering to see the additional AI and automation capabilities."

Ivanti faces competition from two sides of the UEM market: on the one side are those with broad IT portfolios augmenting their UEM offerings and on the other side are those that offer more specialized solutions or aggressive pricing strategies.

Consider Ivanti When

Consider Ivanti for UEM if the IT organization is bullish on AI-driven management of endpoints in a digital employee experience framework. Consider factors like deployment scenarios, integration options, and resource requirements when evaluating Ivanti's solutions against specific needs.

Jamf

Jamf is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Jamf is a device management vendor focused almost exclusively on the Apple ecosystem, providing management and security solutions for Apple devices within corporate, educational, healthcare, and other sectors that have large Mac and mobile estates. Jamf manages macOS PCs (all form factors) as well as iPhones (iOS), iPads (iPadOS), Apple TVs (tvOS), and Apple Watch (watchOS). The vendor has seen strong growth as its expansion has followed the growth of Macs in enterprise environments. (Apple grew 35% in terms of PC shipments in 2022-2023, according to IDC's Worldwide PC Tracker.) Jamf is fast to integration and quick to support new features and capabilities introduced by new iterations of Apple's flagship operating systems. This focus has allowed Jamf to capitalize on the trend of organizations adopting Mac choice programs, transitioning from pilot phases to broader, companywide initiatives. Jamf also integrates with a broad set of enterprise IT systems infrastructure software platforms, such as ServiceNow, Okta, and Microsoft (identity as well as Intune UEM and Sentinel SIEM). The product also has extensive third-party integrations with specific software platforms for electronic health records, school/education classroom management software, and retail POS systems.

From a mobile device perspective, Jamf manages iPads and iPhones with a full UEM feature set and support for capabilities such as user-based administration, multiuser support for iOS/iPadOS devices, and other functions that help support frontline device use cases, such as in hospitals or retail stores. The ability to manage tvOS devices allows Jamf to expand to some IoT use cases, such as managing digital signage and conference room sharing and content management. Jamf also closely followed Apple's recent release of expanded Watch management functionality, allowing the UEM to tightly control settings and features on corporate-owned/managed Apple Watches. From its 2022 acquisition of mobile threat management vendor Wandera, Jamf also has an extensive endpoint security and zero trust network access offering that integrates tightly to Jamf's UEM offering but also supports Windows and Android endpoints.

Strengths

Jamf's deep expertise in managing Apple devices allows for granular control of Macs in enterprise deployments, as well as iPhone and iPad management.

Jamf's strong focus on security, including advanced threat protection and compliance management, aligns with the increasing cybersecurity demands of enterprises.

Jamf's targeted solutions for sectors like healthcare and education allow the company to address use cases tied closely to Apple devices.

Challenges

While Jamf excels in Apple device management, and it has broadened its security capabilities to Windows and Android devices, the Apple-exclusive focus limits the vendor's reach and capabilities in terms of managing broader multi-OS device fleets.

Specific verticals where Jamf has seen success in terms of Mac and Apple device management — such as education — are increasingly adopting non-Apple products, such as Chromebooks in schools, which could limit Jamf's addressable market.

Cost and complexity can be a hinderance to adopt Jamf for some enterprise organizations and among SMBs looking for simple Mac/iPhone management for the cloud. For smaller firms, Jamf has more market-focused offerings, including Jamf Now and Jamf Business Plan, which bundles multiple products.

Consider Jamf When

Jamf's focused strategy on Apple device management, coupled with its extended security and zero trust functionality for other platforms, makes the company a strong choice for enterprises and SMBs looking for granular and comprehensive Mac and Apple mobile device management.

Matrix42

Matrix42 is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Based in Frankfurt, Germany, Matrix42 is a provider of EMM and platforms targeting a wide range of endpoint management use cases with a focus on UEM. The 24-year-old company started in Windows system management and has expanded to EMM/MDM and UEM solutions. It now combines its previously separate Emperium (PCLM) and Silverback (MDM) products into a suite called Matrix42 UEM. The company also offers several key EUC and security-focused products that tie into its UEM offering. Matrix42's IT asset management and service desk products can integrate with UEM to trigger help desk tickets from mobile devices, as well as provision and track devices, apps, software licenses, and other assets associated with an employee or a team. Matrix42 also offers a Windows-based endpoint security product, which can be deployed via UEM and integrates into the UEM dashboard and management console.

Beyond UEM and integrating disparate IT management products, Matrix42 has a larger workspace management strategy, focusing on employee engagement (with measurement/tracking for end-user satisfaction) and AI-based workflow automation (automatically remediating issues with device software, apps, etc.) as well as quick app and user workflow creation capabilities.

Strengths

Matrix42's UEM product has strong support for management features and policy deployment across four major operating systems (Android, iOS, macOS, and Windows) as well as support for the emerging ChromeOS platform.

The UEM dashboard combines data and views across all EUC device types and can also push configuration changes, configuration/policy changes, and apps (mobile and desktop) to all endpoint types.

Matrix42's broader software portfolio can help smaller IT teams converge multiple IT tasks and systems into a single buying center and integrated solution (e.g., teams responsible for all aspects of EUC, including service desk, security, and asset management).

Challenges

Matrix42 has limited support for third-party MTM solutions. MTM support is an increasingly important factor in EMM deployments according to customers interviewed for this IDC MarketScape. Support for third-party CASB and identity platforms was also more limited.

Matrix42 has limited distribution channels and partners outside of Central and Eastern Europe, where it is based. While very strong in this geography, this limits the company in supporting global enterprises.

Consider Matrix42 When

Consider Matrix42 for advanced UEM deployments in midsize to small enterprises, especially among organizations that have already converged PC and mobility management and support teams. Organizations based in the European Union (EU), or with large regional operations in this area, should also consider Matrix42.

Microsoft

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

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.

Microsoft Intune product is part of a broader suite of management, security, and system infrastructure software products tied to its 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.), it has few official partnerships and integrations with third-party products in these areas.

While Intune's reach has expanded into specialized areas of UEM, including Apple management and ruggedized/frontline device management, the vendor 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.

Considering 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 are Windows-first, heterogeneous PC environments with mobile devices function in multiple use cases.

Mitsogo (Hexnode)

Mitsogo (Hexnode) is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Hexnode, based in San Francisco, was founded in 2013, and it currently has approximately 300 employees. With a cloud-based, multi-OS-supporting UEM solution, Hexnode supports Apple (macOS/iOS), Android, and Windows as well as specialized platforms like FireOS and rugged devices. Hexnode UEM focuses on simplicity and easy deployment features, such as zero-touch deployment. Hexnode's strategy hinges on combining a broad feature set with competitive pricing. The UEM solution is designed to be intuitive, reducing the learning curve and operational complexities for users. This approach particularly appeals to small and medium-sized businesses and enterprises with small IT teams looking for cost-effective UEM capabilities.

While supporting the four major device operating systems, Hexnode has a particular focus on Apple, with support for advanced Mac management features (custom macOS app delivery and automated Mac enrollment) as well as support for new macOS and iOS features quickly after new releases of the operating systems are available. It also supports Apple Business Manager enrolment and bulk app purchasing and user-based iOS enrolment. While Hexnode is an Apple-focused UEM provider, it does not exclusively support macOS/iOS devices. Its breadth across Windows, Android, and Chrome will be attractive to firms with Apple management needs, but with broader endpoint support requirements.

Strengths

Multi-OS support and zero-touch deployment is a strength for Hexnode UEM. The platform can manage a wide array of operating systems and its zero-touch deployment feature significantly reduces IT workload.

Hexnode's UEM platform has a unified, intuitive console for IT professionals and enhances user experience and reduces the time spent on training, thereby increasing productivity.

Catering to a wide range of businesses, Hexnode's pricing strategy is flexible and competitive, making it accessible to small businesses while offering the features and scalability required by larger enterprises.

Challenges

Hexnode will find it difficult to match the capabilities of those specializing in single-OS UEM solutions, particularly for Apple devices. While this underscores the need for Hexnode to continue innovating and differentiating its offerings, it also presents an opportunity as companies add more Apple devices, specifically Macs, and bring existing Mac devices under management.

While Hexnode has strong offerings, attractive pricing, and delivery models for SMBs, it does not partner with many carriers and mobile operators, which are still channels for reaching SMBs, especially for mobile device management use cases.

Consider Mitsogo (Hexnode) When

SMBs and enterprises with lean IT/support teams should consider Hexnode's UEM product for multi-OS support, with a focus on cloud-based Apple device management. The vendor's flexible, competitive pricing and simple rollout capabilities are also strong points to consider.

OpenText

OpenText is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

OpenText now competes in the UEM market based on its acquisition of Micro Focus in January 2023. OpenText's UEM product, ZENworks, provides strong device and application management functionality across PC, mobile device, and IoT endpoint form factors, covering all major operating systems (Windows, macOS, iOS/iPadOS, Android). The product emphasizes ease of deployment, integration with a range of other OpenText IT infrastructure software platforms, and user-friendly interfaces. Key features include advanced security measures, flexible management options, and support for a wide range of devices. In addition, the company's strategy, strengths, and weaknesses in the context of market competition and product development are highlighted. The full transcript contains valuable details for a deeper understanding of OpenText's approach to UEM with ZENworks.

OpenText's acquisition of Micro Focus brings several advantages and impacts on the ZENworks UEM product and its market opportunity. The acquisition enhances cloud capabilities, leveraging OpenText's strong presence and infrastructure in cloud services. This transition supports ZENworks' evolution into a more cloud-friendly, containerized platform, addressing a critical need for SaaS solutions among customers. The integration of OpenText's endpoint security capabilities, like Webroot and Carbonite, into ZENworks strengthens its endpoint management and security offerings. Overall, the acquisition positions ZENworks favorably in the competitive UEM market, particularly in cloud and AI integration, expanding its market opportunities.

Strengths

Post the OpenText acquisition, ZENworks is focusing on enhancing cloud capabilities, leveraging OpenText's expertise in cloud services and infrastructure.

The integration with OpenText's security capabilities (like Webroot, BrightCloud, and Carbonite) enhances ZENworks' endpoint security and backup solutions.

ZENworks is incorporating AI, aiming to leverage OpenText's AI capabilities, such as natural language processing and predictive analytics, to enhance endpoint management and security.

Challenges

While OpenText is focusing on cloud integration, there is a segment of the traditional ZENworks customer base that is cautious or slow in transitioning to the cloud.

Brand recognition and association, especially across varying customer bases, remain a challenge for OpenText post-acquisition. The vendor is still in the process of integrating and aligning different products and services into a cohesive platform/portfolio offering.

For a vendor with strong focus on SMB and midmarket UEM, OpenText has fewer carrier/mobile operating partnerships. Carriers are still seen as a primary channel for reaching UEM/MDM customers in the midmarket.

Consider OpenText When

OpenText's ZENworks UEM platform covers multi-OS end-user computing device management use cases and can also address specialized management scenarios such as ruggedized and IoT endpoint management. Firms looking for strong Windows management primarily, with expansion into particular SMBs or enterprises with small IT staffs looking to consolidate product functionality and vendor sourcing, can benefit from the multiple functionalities ZENworks UEM offers in a single console, as well as complementary security and management products offered across the OpenText portfolio.

Quest

Quest is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Quest Software has made significant strides in the unified endpoint management market through its Quest UEM and KACE products. These offerings are designed to address a broad set of PC and mobile device management use cases in enterprises and SMBs, especially for firms with smaller IT staffs looking to integrate dashboards, tools, and consoles. Quest's strategy centers on providing a comprehensive, flexible, and security-focused UEM solution. The company emphasizes endpoint security, flexibility, and integration capabilities, coupled with an enhanced user experience to navigate the complex landscape of endpoint management. This strategy is bolstered by ongoing product enhancements, such as the inclusion of remote desktop capabilities and a focus on simplifying workflows and providing actionable business insights. Quest has added this capability to its already strong array of ruggedized endpoint management features. From a Windows device management perspective, Quest has deep integration with Windows policy and compliance controls, with extensive management capabilities for Windows devices. Small and medium-sized businesses also benefit from Quest's flexibility and scalability and broad product portfolio for systems infrastructure software.

Strengths

Quest UEM and KACE offer robust support across a variety of platforms, including Windows, Mac, Linux, iOS, and Android, addressing the needs of a distributed workforce and enabling remote desktop access and mobile device management.

Quest's built-in UEM security functions complement the company's portfolio of products, which extend to penetration testing, threat detection, and proactive remediation capabilities, to protect against vulnerabilities and ensure compliance.

Quest supports hybrid deployment models and offers extensive integration options with digital workplace tools and third-party applications, facilitating a seamless IT ecosystem.

Challenges

While not only a Windows management specialist, Quest competes in a competitive Windows device management space. Quest must position its solutions to not only complement but also enhance the value offered by large incumbent Windows device management platforms.

Mobile carriers are a key channel for reaching SMBs with UEM and mobility products in particular. While Quest has strong functionality and bundling, which is attractive to SMBs, it has fewer partnerships among mobile carriers than other SMB-centric UEM vendors.

Consider Quest When

Enterprises with lean IT staffs, as well as SMBs, should consider Quest Software's UEM for its comprehensive management capabilities, robust security features, and flexible deployment options. Quest's strategic focus on integration, security, and user experience positions the company well in the UEM market.

Samsung

Samsung is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Samsung, a global consumer and mobile technology company, has made significant strides in the unified endpoint management market with its Samsung Knox Manage product, part of the broader Knox Suite — a broad-reaching set of solutions targeting the management, support, and security of Samsung Android devices, as well as non-Samsung multi-OS endpoints. Samsung's primary approach to UEM is attaching its strong brand reputation to deliver UEM as an add-on solution for small or large deployments of Samsung devices. Knox Manage, a cloud-based product, provides deep integration with Samsung hardware and underlying device-side Knox security APIs and functions added to the Samsung version of Android. Strong carrier relationships, and its position as the dominant smartphone brand worldwide, have led to strong deployments in enterprises, especially among industries such as manufacturing, transportation, retail, and other verticals with frontline and dedicated device use cases.

While Android first in nature, Knox Manage does support Windows and Apple devices, with MDM-based functionality to manage Windows 10/11 and macOS endpoints. The product also supports iOS/iPadOS endpoints via MDM protocol controls. Samsung also excels in managing frontline devices, both Samsung branded and other devices based on standard Android technology. Knox Suite provides robust features tailored for frontline and field workers who require durable and secure devices. Knox Manage is designed to be accessible and useful for SMBs, with scalable solutions that can grow with the business, and a brand carried by a large number of mobile carriers worldwide — a primary channel for SMBs buying mobility solutions.

Strengths

Samsung's deep hardware integration with Samsung devices provides tightly integrated management, security, and analytics features for large device fleets of Samsung smartphones and tablets, used widely by large enterprises and other organizations. This focus on security, including secure boot and real-time protection, makes the platform a strong choice for organizations prioritizing device security.

Among all UEM vendors, Samsung has a broad set of mobile operator partnerships for reselling devices and UEM services. Operators are a key channel for reaching SMBs, as well as enterprises with extensive cellular connectivity and mobility needs.

Samsung's broad cloud-delivered UEM offering allows for strong support and coverage for mobile workers in frontline and field use cases as well as for traditional mobile workers.

Challenges

Samsung does not have a portfolio of complementary IT infrastructure software products (e.g., ITSM, endpoint security, networking, server management).

While strong in Android device support and functionality, the most differentiating features and capabilities (such as over-the-air firmware upgrades and deep device analytics) are only limited to Samsung Android endpoints managed by the broader Knox Suite.

Consider Samsung When

Organizations with growing fleets of Samsung Android devices should consider Samsung Knox Manage for its strong security features, deep hardware integration, device performance analytics, and comprehensive device management capabilities. Businesses should also consider Knox Manage as a full UEM if there is a need to support PCs and Apple devices with cloud-based MDM protocol management functionality. Many firms with other UEMs in their environments deploy Knox Manage specifically for its Samsung-centric functionality.

Sophos

Sophos is positioned in the Major Players category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Sophos, a prominent and longtime cybersecurity vendor, has made significant strides in the unified endpoint management market with its Sophos UEM product. This product is part of Sophos' broader portfolio, which includes managed detection and response (MDR) and firewall solutions, catering to a wide range of customers from small businesses to large enterprises. Sophos' UEM solution is designed to streamline the management and security of devices across an organization, offering features such as device enrollment, application management, and security policy enforcement.

Sophos' approach to the UEM market leverages the company's strengths in cybersecurity, a strong global presence, and a deep understanding of customer requirements for integrating management and monitoring systems. In terms of Apple device management, Sophos aims to provide robust management solutions that rely on MDM protocol management for Mac and iOS/iPadOS users. For Windows device management, Sophos leverages its extensive experience in endpoint security to expand its capabilities to modern Windows endpoint management functions. In line with its longtime market approach and positioning, Sophos is focused particularly on serving small and medium-sized businesses by offering an integrated UEM product that ties into a larger, singular security platform.

Strengths

Sophos' prowess in cybersecurity, and the company's extensive partner ecosystem in security, provides the vendor strong technology and selling platforms for expanding its UEM presence. This allows Sophos to deliver UEM solutions to a wide range of customers, especially among managed service providers bundling UEM with the vendor's MDR offering.

Tight integration of Sophos UEM to the broader Sophos security product portfolio sets up users to deploy a range of automations and triggered actions based on security detections. This is particularly valuable for small IT staff that rely on single-vendor integrated systems to streamline management and security tasks.

Challenges

While Sophos has strong UEM capabilities for standard end-user PC/mobile computing needs, the vendor has fewer capabilities for supporting specialized UEM use cases, such as frontline worker scenarios, ruggedized/IoT UEM management functions, and emerging use cases such as wearable and augmented reality/virtual reality (AR/VR) device management.

The strong tie-ins between Sophos UEM and the vendor's broader security product portfolio are a great benefit to "all-in" Sophos customers, but less so for customers using other vendors as their primary cybersecurity product supplier.

Consider Sophos When

Customers should consider Sophos UEM for its focus on cybersecurity and ease of use and a unified management console. The ability of the vendor to address the specific needs of different customer segments, coupled with its global presence and strong partner ecosystem, makes Sophos a strong choice for businesses looking to consolidate endpoint management and security tools and operations.

SOTI

SOTI is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

Canada-based SOTI has been in the MDM/UEM market for over 15 years. MobiControl is SOTI's flagship product. It is a comprehensive device management solution catering to a variety of industries with a specific focus on frontline, ruggedized, and deskless worker device use cases. The product's main strength lies in its ability to manage, support, and secure a vast array of mobile devices and IoT endpoints. MobiControl offers features like remote control, location tracking, and content management. One of the few remaining large standalone EMM/UEM vendors in the market, SOTI has wide adoption for EMM of computing endpoints deployed in environments such as warehouses, factories, and airports, as well as in field services, retail, and medical scenarios. The SOTI MobiControl product is the main UEM offering providing MDM, MAM, and MCM capabilities from a single code base via on-premises or cloud-delivered software. While some SOTI customers interviewed for this study used MobiControl for all mobility use cases, several others said they used MobiControl to manage legacy and modern ruggedized devices, as well as other user-interfacing IoT-like endpoints, alongside another third-party EMM solution for other mobility use cases.

Strengths

While known for ruggedized and IoT mobile endpoint management, SOTI has supported macOS since 2018. It has extended this capability to include support for deploying apps, enforcing configuration settings (e.g., Wi-Fi and VPN settings), and enrolling in-device inventory and monitoring functions via SOTI's UEM platform.

SOTI's strength is the breadth of device types the company supports – from legacy Windows CE, NT, and XP platforms to Linux devices, bar scanners, mobile printers, and other ruggedized single-purpose devices and smartphones. This has led to many customers using SOTI specifically for management of these types of devices, even with the presence of another EMM platform.

SOTI's MADP and mobile help desk capabilities are unique. SOTI does not have to partner with other specialist vendors, or integrate products from separate business units, to approach such an offering.

Challenges

While well recognized in ruggedized and field service mobile technology deployments, SOTI is not as widely known for supporting traditional mobile knowledge workers, which is a much larger addressable market in terms of growth and potential seat expansion.

SOTI has outlined larger ambitions in product road map briefings around larger IoT initiatives, mobile application development, and rapid app dev solutions, as well as worker productivity apps, but it has not fully delivered on these initiatives or articulated a larger strategy for the company.

SOTI has limited partnerships and support with other third-party identity and cloud application security broker technologies, limiting the ability to support cloud-based SSO or integrations with other identity platforms.

Consider SOTI When

Consider SOTI when your organization requires management, security, and policy control over a wide range of ruggedized mobile devices, legacy OS devices, or specialty handheld devices and peripherals. Small to midsize enterprises with ruggedized devices may consider SOTI for all UEM device deployments. Larger enterprises with ruggedized/IoT needs may consider SOTI as a separate solution for those specific use cases.

Zoho (ManageEngine)

Zoho (ManageEngine) is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide UEM software for frontline/IoT devices.

ManageEngine is the IT infrastructure software division of Zoho, a global cloud software and business application development company based in India. The United States-based ManageEngine has been in business for over 20 years, with a wide array of management and security products, including its ManageEngine UEM product. ManageEngine UEM combines multiple-OS management functions (Windows, Mac, iOS, Android, ChromeOS, and Linux) with ties to other key IT infrastructure products in the vendor's portfolio (including endpoint security, IT service management, server management, and identity tools). Zoho/ManageEngine's UEM approach involves creating custom workflows to meet unique business requirements, embedding AI into the platform for enhanced administrative assistance, and proactive IT administration and security.

Windows device management is a heritage strength of ManageEngine, with strong configuration and policy management capabilities coupled with tools such as CIS compliance templates. The product also provides broad Apple Mac management functionality with MDM-based and agent-based capabilities for macOS enrollment, policy enforcement, and life-cycle management. Device management for small and medium-sized businesses is also a strong suit for Zoho/ManageEngine. Its UEM product's scalability and extensive policy automation make it good fit for organizations looking to consolidate multiple endpoint management and security functions. Nontraditional endpoints are also well supported by ManageEngine UEM — wearables (Google Glass, Microsoft HoloLens), ruggedized devices (Zebra, Honeywell, Datalogic devices), and IoT endpoints (i.e., Apple TVs).

Strengths

ManageEngine UEM has comprehensive endpoint management and security features that cater to a wide range of devices and operating systems.

Zoho/ManageEngine is working to integrate AI into its integrated workflows, allowing for proactive incident prevention and configuration management.

The vendor has a global presence and can scale from SMB customers to very large enterprises.

Challenges

Zoho/ManageEngine has fewer compliance certifications (governmental and vertical industry) than some of its larger, leading market competitors serving the enterprise market.

Zoho/ManageEngine must further expand the opportunity to leverage the global Zoho software brand and link it more tightly to the ManageEngine IT infrastructure division. The vendor has started to do this, but more go-to-market and cross-selling activity needs to happen to take this further.

Consider Zoho (ManageEngine) When

Companies seeking a UEM solution that ties together with a broader portfolio of IT infrastructure and security products should consider Zoho/ManageEngine for its comprehensive endpoint management capabilities and strategic focus on AI and automation. The company's approach to addressing the needs of diverse IT environments makes Zoho/ManageEngine a strong choice, especially for organizations looking to converge security and management platforms and teams.

Vendors to Watch

Every IDC MarketScape cycle results in vendors that do not qualify for inclusion in the study. For many vendors, either it is too early in their life cycle, they are undergoing product transitions, or they are simply too small. For this IDC MarketScape, these are the vendors to watch:

- **Barramundi Software:** It is a German-based UEM vendor with a focus on automation and integration of endpoint device management with its portfolio of network management, IoT management, server management, and security products.
- **CrowdStrike:** A large enterprise endpoint security software vendor, CrowdStrike launched its first UEM product in March 2024, with capabilities for Windows, macOS, and Linux device enrollment, configuration management, and software patching, tied closely to the vendor's larger Falcon endpoint detection and response (EDR) platform used widely by large enterprises.

- **Fleet:** Fleet is an open source endpoint management platform supporting Windows, macOS, and Linux and expanding to mobile device OSs in 2024. The data-centric platform is targeted at firms with large device fleets and provides APIs for automating software pushes to endpoints and the pulling of data from managed devices (for ingesting into SIEM or other analytics tools).
- **HMD:** The former device-making arm of Nokia, Finland-based HMD makes consumer and business mobile devices and offers Enable Pro, an enterprise mobility management solution based on Android. A console gives IT departments tools to enroll and centrally manage any Android-based smartphones or tablets.
- **Scalefusion:** Headquartered in Pune, India, Scalefusion offers a cloud-based UEM platform that manages Windows, Mac, Android, iOS, and Linux endpoints. It provides reporting and analytics features, security compliance templates, and other tools for SMB/midmarket IT organizations with large, mixed-OS device fleets.

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.

Strategies and Capabilities Criteria

To assess vendors, IDC collected and analyzed data based on two major axes – strategy and capability. In evaluating vendors, IDC considered vendor RFI responses and demos, customer/partner references, surveys, and accumulated vendor and market insights.

Tables 1 and 2 present the strategies and capabilities criteria, respectively.

TABLE 1

Key Strategy Measures for Success: Worldwide Unified Endpoint Management Software for Frontline/IoT Devices

Strategies Criteria	Definition	Weight (%)
Customer strategy rating	The vendor's customer-facing delivery capabilities satisfy market wants and create a strong level of value for its customers.	5.0
Financial/funding	The company will generate, attract, and manage capital well over the next three to five years to create market value.	11.0
Functionality or offering strategy	The vendor's current development of offerings will be relevant and attractive to customers over the next three to five years.	5.0
Growth	The vendor's capabilities maximize the connection between offerings and customers, such as delivery, partnerships, pricing, distribution, marketing, sales, and service.	45.0
Innovation	The pace of continued investment is expanding the company's industry cloud offerings over the next three to five years.	12.0
Pricing strategy	The vendor is willing to demonstrate value through flexible pricing mechanisms.	8.0
R&D pace/productivity	The vendor is investing strategically in new technology, capabilities, and products to meet customers' future needs.	14.0
Total		100.0

Source: IDC, 2024

TABLE 2

Key Capability Measures for Success: Worldwide Unified Endpoint Management Software for Frontline/IoT Devices

Capabilities Criteria	Definition	Weight (%)
Customer capability rating	Customers of the vendor rate its capabilities high and as meeting their needs.	5.0
Delivery model	The delivery model for the product as well as associated support and maintenance services is well positioned for future customer needs, and it aligns with market trends.	5.0
Functionality or offering	The features and capabilities of the vendor's product meet the current needs of customers.	62.0
Integration capabilities	The product has strong technical integration capabilities with relative adjacent portfolio and external partner solutions.	9.0
Portfolio benefits	The vendor has a strong portfolio of adjacent and complementary products and services relative to the main product being analyzed in this study.	15.0
Range of services	The vendor offers a strong range of services in support of the product offering.	4.0
Total		100.0

Source: IDC, 2024

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 represents a vendor assessment of the unified endpoint management software for frontline/IoT device deployments through the IDC MarketScape model.

"Frontline endpoints and IoT devices are often the tip of the spear in terms of digitally transforming business operations and processes," says Phil Hochmuth, research VP, Endpoint Device Management and Enterprise Mobility, IDC. "UEM tools can help enterprises ensure devices used by deskless workers, shift employees, and mobile/field workers are secure, as well as properly configured and provisioned, positioning workers for higher productivity and efficiency."

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