Drastic change and a global pandemic marked a tumultuous year in the UEM market. The past 12 months magnified legacy CMT limitations and drove I&O leaders to UEM for reduced complexity, location-agnostic device management and analytics to track and improve device performance and user experience.

**Strategic Planning Assumption**

By 2024, more than half of organizations will consolidate to a single console for endpoint management and security tasks, up from less than 5% in 2020.

**Market Definition/Description**

Gartner’s view of the unified endpoint management (UEM) market is focused on transformational technologies or approaches delivering on the future needs of end users. It is not focused on the market as it is today.

Gartner defines the UEM tools market as a set of offerings comprising mobile device management (MDM) and management of personal computers, via traditional client management tools (CMTs) or modern management, through a single console that also combines the application of data protection, device configuration and usage policies. Modern UEM tools:

- Provide a user-centric view of devices across device platforms.
- Enable modern PC management through native Windows 10, macOS and Chrome OS controls.
- Enable MDM through native iOS and Android controls.
- Aggregate analytics and telemetry from users, apps and devices to help inform policy and related actions.
- Provide insights into user experience through aggregation of telemetry signals, events, logs and synthetic transactions.
Integrate with unified endpoint security (UES) tools to support security policy management, execute administrative actions and improve integration with identity and access management (IAM) tools.

Additionally, UEM offers direct management of nontraditional devices including Internet of Things (IoT) devices and wearables; however, Gartner does not deem these extensions to be core to the market.
Magic Quadrant

Figure 1. Magic Quadrant for Unified Endpoint Management

Source: Gartner (August 2020)
Vendor Strengths and Cautions

BlackBerry

BlackBerry is a Challenger in this Magic Quadrant. Its BlackBerry UEM product is focused on providing secure access to data, apps and workspaces from any device. Its operations are geographically diversified. Its clients tend to operate in highly regulated mobile markets in North America and Europe (e.g., government and financial services). BlackBerry continues to invest in a comprehensive endpoint security and management product, improved Microsoft Graph integration, and expanded AI-based controls.

Strengths

- **Highly secure**: BlackBerry’s core strength is delivering a highly extensible, secure personal information management (PIM)/container to regulated markets, backed by an extensive list of certifications. This is underpinned by a strong zero trust framework that enables frictionless, continuous user authentication to help customers address the often-conflicting goals of reducing security risk and improving the user experience with technology.

- **Workspace**: BlackBerry Digital Workplace (via partnership with Awingu) securely delivers third-party-hosted virtual applications and desktops to company-owned and personally owned devices. Many customers have indicated that this was a critical success factor in their ability to rapidly support remote work in response to the pandemic.

- **UEM plus UES**: BlackBerry is one of only two vendors in this Magic Quadrant that offers a complete UES solution. Cylance directly integrates with the PIM container, adding an additional level of security for managed and unmanaged devices.

Cautions

- **Limited PC management**: While strong with MDM, BlackBerry’s UEM provides only basic Windows 10 and minimal macOS management capabilities. Traditional CMT functionality is available only through coexistence with Microsoft Endpoint Configuration Manager; however, BlackBerry does not provide this integration. It does provide functionality to help migrate to modern OS management.

- **Platform strategy**: BlackBerry’s endpoint strategy promotes a platform play centered on security, workspace and mobility. Gartner’s analysis of social media activity reflects conversations about BlackBerry’s relevance shifting from UEM toward security.

- **Microsoft 365**: BlackBerry customers that also subscribe to Microsoft 365 face increasing pressure to reduce costs associated with paying for two UEM solutions. BlackBerry’s ability to fulfill highly regulated market requirements allows it to retain its installed base; but if Microsoft can meet those requirements in the future, BlackBerry could face extensive customer attrition.
Citrix

Citrix is a Niche Player in this Magic Quadrant. Its Citrix Endpoint Management (CEM) product is focused on providing a digital workspace (endpoint management, content collaboration and virtual app/desktop). Its operations are geographically diversified, and its clients tend to be small to midsize enterprise organizations in government, healthcare and financial services. Beyond core UEM, key investments include analytics, zero trust, improved frontline support and tighter third-party security integration.

Strengths

- **Workspace**: Citrix Workspace offers a contiguous solution for device management, and hosts and delivers virtualized applications or desktops from a single management console. This seamless integration simplifies the IT admin experience and improves user experience.

- **BYOD**: Citrix’s containerized applications can be run on an unmanaged device and are routinely praised for usability by organizations using them. For Microsoft customers, Citrix apps can be managed using either Citrix Workspace or Microsoft’s mobile application management (MAM) controls and integrations.

- **Nontraditional devices**: Citrix provides rich support for its Citrix Ready workspace hub and workplace IoT devices, using orchestration to reduce the complexity of connecting to shared infrastructure devices and workspace hardware. Gartner client feedback and social media analytics highlight satisfaction with real-time location service capabilities and enhanced user experience, especially for frontline worker use cases.

Cautions

- **Platform value proposition**: Gartner rarely sees clients consider buying CEM as a stand-alone UEM; rather, it is usually part of a larger Citrix infrastructure offering. This aligns with the Citrix workspace go-to-market strategy.

- **Modern management limitation**: Citrix’s management of Windows devices lacks rich CMT migration functionality unless the Citrix Workspace Environment Management (WEM) module is used.

- **Long-term strategy**: While CEM currently supports Windows 10 modern management, its long-term strategy is to complement Microsoft Endpoint Manager for additional Windows 10 management capabilities.

IBM

IBM is a Leader in this Magic Quadrant. Its IBM Security MaaS360 with Watson product is focused on artificial intelligence (AI)-enhanced UEM. Its operations are geographically diversified, and clients tend to be small to midsize technology, retail and manufacturing companies based in the Americas and Europe. IBM continues to invest in AI, ensuring alignment with new devices, features and use cases, and deeper integration with identity and endpoint security products.
**Strengths**

- **Watson Analytics:** IBM has used its Watson AI expertise to deliver analytics designed to help customers identify, prioritize, triage and resolve issues on devices managed by MaaS360. Customers value the efficiencies gained from customizable, automated reporting that helps them identify and prioritize critical issues.

- **Ease of use:** Gartner clients continue to report that MaaS360 is easier to implement than other UEM solutions. The product offers several policy templates through a wizardlike interface that uses AI to deliver benchmarked reports that enable customers to configure and validate their environment against peer and published practices. It also has a clean dashboard to react to events quickly.

- **Strong CMT support:** The integration with third-party CMTs, along with Group Policy Object (GPO) migration capabilities, simplifies the journey to co-management and modern management. Clients have referenced positive experience with integrations to Microsoft Endpoint Configuration Manager, HCL BigFix and Tanium. IBM also offers self-directed patching and application updates for Windows and macOS (using OPSWAT), and tools to help customers migrate to modern management.

**Cautions**

- **SaaS only:** MaaS360 is available only as a SaaS solution and does not provide any on-premises management option. It does, however, offer an on-premises access gateway to enable mobile devices to access email and other applications.

- **Mostly midmarket:** Gartner rarely sees MaaS360 on enterprise client shortlists unless the organization is already heavily invested in IBM software. IBM is working on enabling its sales force to sell MaaS360; however, most sales are from small to midsize companies or through the carrier channel.

- **Limited endpoint diversity:** Despite strong CMT integration, most clients report using MaaS360 to manage mobile devices rather than as UEM to manage PCs via co-management or modern management.

**Ivanti**

Ivanti is a Challenger in this Magic Quadrant. The Ivanti Unified Endpoint Manager product continues to extend its proven client management capabilities as it transitions into modern management and a single pane of glass across endpoint management. Its operations are geographically dispersed. Its clients tend to be midsize enterprise organizations. Ivanti continues to invest beyond UEM capabilities with integrated security, analytics, automation, self-healing and robust, real-time discovery capabilities.

**Strengths**

- **New leadership and UEM focus:** Ivanti participates in several markets, but its new executive leadership team brought in during 1Q20 has publicly commented that UEM will be one of
Ivanti’s two strategic focuses moving forward. To drive awareness and interest, the new leadership hosted a series of pandemic response webinars, offered free trials of its software, prioritized solutions and guidance to support frontline healthcare workers, and invested heavily in a new partner portal.

- **Sales model**: Ivanti’s refocus on its direct sales model will improve the company’s ability to directly engage with customers moving forward. Traditionally, Ivanti has relied on channel-based sales. New product bundles and pricing helped drive its improved installed base.

- **Cloud and automation expansion**: Ivanti continues to expand its Neurons platform to provide self-healing, analytics and real-time intelligence delivered via dashboards, as well as a natural language search to support initiatives such as device migrations and health assessments. The recent addition of cloud storage and a content delivery network extends endpoint management, patching, and application deployment for remote workers without requiring a VPN.

### Cautions

- **Limited MDM**: Ivanti’s long-term focus on client device support has limited its development of mobile device, content, application and identity management capabilities. Functionality and client interest lag the competition. Gartner rarely sees Ivanti on clients’ UEM shortlists for scope that extends beyond client management.

- **Legacy naming**: Continued client references to the LANDesk naming and a lack of awareness of the Ivanti value proposition and differentiators highlight messaging gaps.

- **Portfolio consolidation**: Though Ivanti is actively working on portfolio consolidation, Gartner clients often voice concerns about using multiple products and are generally unaware of Ivanti’s overall endpoint management and SaaS offerings.

### Microsoft

Microsoft is a Leader in this Magic Quadrant. Microsoft Endpoint Manager (MEM) combines Intune and Configuration Manager and is available with an Enterprise Mobility + Security (EMS) license. Microsoft’s operations and clients tend to be geographically diversified. Microsoft continues to invest in improving end-user and IT admin experience, integration with endpoint security and identity systems, and expanded use of analytics, AI and machine learning (ML).

### Strengths

- **Marketing and product strategy**: With the establishment of MEM, Microsoft offers the most used UEM tool on the market, with significantly more devices under management than its competition. Though many I&O leaders are confused by the MEM, Configuration Manager and Intune relationship, online references in 4Q19 increased by 278%, with discussions on how MEM combines its offerings into a single console at no additional cost.

- **Microsoft native**: Deep integration across Microsoft products offers security capabilities that are difficult to replicate piecemeal. Evidence of improved stability and performance achieved by
Reducing third-party plug-ins cannot be ignored. MEM’s integration with Azure Active Directory, Defender Advanced Threat Protection (ATP) and Microsoft 365 app protection offers improved security and user experience through zero trust conditional access.

- **Co-management:** Improved Intune and Configuration Manager integration, along with the pandemic, have accelerated adoption of co-management and modern management. Prepandemic, clients were too focused on replacing Windows 7 with Windows 10 to adjust their endpoint management strategies.

**Cautions**

- **Third-party integrations:** Clients frequently struggle with limited integration with third-party identity, service and asset management, and endpoint security products. Additionally, organizations seeking advanced macOS management and remote control are required to use third-party integrated solutions.

- **Nonstandard use cases:** MEM currently lacks robust management capabilities for IoT, wearables, rugged frontline devices and UNIX/Linux operating systems as well as required controls for highly regulated use cases where containerization and integrated VPNs are more common. MEM enables management of Microsoft 365 Enterprise apps and data using Intune app protection policies and conditional access; however, that may not meet compliance requirements.

- **Difficult to use:** Clients’ most common concern is that using MEM is not easy. Reasons include the overhead required to architect, build and maintain Configuration Manager and integration between on-premises Active Directory (AD) and Azure AD. Managing some policies (like Windows Hello) requires use of multiple consoles. Clients also frequently voice frustration with staying abreast of product updates and finding documentation and best practices across the various websites, communities and blogs.

**MobileIron**

MobileIron is a Visionary in this Magic Quadrant. Its UEM product is focused on UEM and secure access for both on-premises and SaaS applications. Its operations are geographically diversified. Its clients tend to be enterprise organizations in the Americas and Europe. MobileIron continues to invest in increasing the value of endpoint security, macOS and frontline worker capabilities.

**Strengths**

- **Zero sign-on:** MobileIron Access complements the core UEM offering to enable a zero trust security posture based on user identity, app-level trust and device telemetry. The combined capability enables passwordless authentication, which MobileIron calls “zero sign-on (ZSO).” MobileIron Threat Defense (via partnership with Zimperium) adds an additional layer for zero-day protection against device, network, application and phishing attacks.

- **Expanded macOS support:** MobileIron expanded its macOS functionality to support distribution of custom packages (.app, .dmg, .pkg formats) outside of the Mac App Store. In addition, the tool supports retrieving custom device attributes (for example, Java Development
Kit [JDK] versions) and specifying application dependency requirements (for example, require an endpoint protection platform before application installation).

- **Extensive use cases:** MobileIron AppStation enables organizations to distribute apps to an extended workforce, such as contractors, frontline workers or part-time employees, to allow secure corporate access when devices cannot be enrolled. Combined with OEM-specific support for Zebra LifeGuard, Zebra OEMConfig and Samsung Knox in addition to zero touch enrollment, this feature aims to enhance frontline worker productivity.

**Cautions**

- **Value proposition:** As competitors expand their UEM suites to bundle support for virtual desktop infrastructure (VDI)/desktop as a service (DaaS) and unified endpoint security, MobileIron’s value proposition as a stand-alone UEM product comes under increased scrutiny.

- **Functional disparity:** The on-premises MobileIron Core is not as robust as MobileIron Cloud. For example, the admin portal lacks a customizable timeout, forcing users to log in multiple times a day.

- **Endpoint analytics:** Although MobileIron UEM includes reporting and dashboards for compliance verification, and integrates with Splunk, it lacks broader endpoint and workplace analytics to help IT admins identify and address device performance and user experience issues.

**Sophos**

Sophos is a Niche Player in this Magic Quadrant. Its Sophos Central product is broadly focused on a combination of UEM with UES. Its operations are geographically diversified, and its clients tend to be small to midsize enterprise organizations based in Europe and North America. Sophos continues to invest in simplifying customer migrations from on-premises to SaaS, strengthening capabilities to manage Windows 10 and macOS, and integrating endpoint management and endpoint security products.

**Strengths**

- **UEM plus UES:** Having integrated its own security and management products, Sophos demonstrates more maturity in the integration of endpoint management and endpoint security functionality. Its own data lake of device configurations and activity enables continually updated risk profile information for UEM-managed devices, including behavior of applications and application subelements (such as libraries, API calls, etc.).

- **Growing customer base:** Traditionally a midmarket leader, Sophos has broadened its appeal by streamlining its products, adding broader security controls through acquisition and refreshing its marketing. This is evidenced by an increase in its average installed base and deal size.
- **Strong data containment:** Sophos Central includes Secure Workspace for secure document access and a corporate browser. It also includes Sophos Secure Email (via partnership with Virtual Solution), which offers an easy-to-use interface and runs as part of the Sophos container.

**Cautions**

- **CMT integration:** Sophos continues to exhibit a modest level of CMT functionality in its product and on its feature roadmap. It only integrates with Materna DX-Union, but does offer agent-based migration and basic Windows and macOS modern management capabilities.

- **Limited endpoint diversity:** Although Sophos offers modern management, clients report using the tool solely for management of mobile devices and not PC or Mac management.

- **Brand awareness:** Sophos is rarely seen on shortlists from Gartner clients for device management. This is often related to lack of brand awareness outside of the traditional endpoint protection platform security space where the company is well known.

**VMware**

VMware is a Leader in this Magic Quadrant. Its Workspace ONE product is focused on providing improved employee experience through UEM, virtualization, analytics, apps and workflows. Its operations and clients tend to be geographically diversified. VMware continues to invest in helping customers drive workplace modernization, implement zero trust and improve employee experience, anchored by Workspace ONE Intelligence and Carbon Black endpoint security integration.

**Strengths**

- **End-to-end solution:** VMware enables remote work and a seamless, device-agnostic user experience through its deep integration of UEM with single sign-on (Workspace ONE Access), remote access (Workspace ONE Tunnel), endpoint security (Carbon Black), and desktop and application virtualization (Horizon); and support for many third-party solutions. Social media analytics highlight satisfaction with the remote onboarding feature, which has taken on increased importance during the COVID-19 pandemic.

- **Ease of use:** VMware offers seamless integration of traditional and modern PC and mobile management techniques through the same console, in addition to in-console templates and wizards to empower IT admins to maximize value. VMware also curates a vast online knowledge repository that includes product information, videos, labs, blogs, implementation guides, learning activity paths and reference architecture in its Tech Zone portal.

- **Flexibility:** VMware’s flexible architecture enables customers to operate exclusively on-premises, exclusively in SaaS, or a hybrid of the two where customers decide on a component level what model is a best fit. Standard and customizable connectors can enable complex integrations. VMware also offers several integrations with third-party identity, endpoint security, IT operations and IT service management tools.
Cautions

- **Platform value proposition:** To maximize the unique value of VMware’s Workspace ONE platform (e.g., employee experience, risk-based conditional access [zero trust], automation, intelligence and analytics, etc.), clients will need to purchase the Enterprise license tier.

- **Advanced feature adoption:** VMware continues to make investments in areas such as modern management of Windows and macOS devices, and offerings such as employee onboarding; yet adoption has been slower than expected.

- **Microsoft 365:** VMware customers committed to Microsoft 365 must rationalize the incremental cost of paying for Workspace ONE and Microsoft Endpoint Manager, or should look for advanced Workspace ONE capabilities to complement Endpoint Manager. The Workspace ONE integration to MEM offering is currently in limited beta.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor’s appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

**Added**
- Sophos

**Dropped**
- 42Gears
- ManageEngine
- Matrix42
- Snow Software

Inclusion and Exclusion Criteria

For Gartner clients, Magic Quadrant research identifies and then analyzes the most relevant providers and their products in a market. To qualify for inclusion, vendors must present a defensible solution capable of the following:

1. A currently shipping, single license product that demonstrates:
   - Mobile device management:
     - Apple (iOS and iPad OS)
Android (including Android Enterprise)

Modern management of Apple macOS and Windows 10, which includes:

- Device enrollment and provisioning (Windows Autopilot and Apple Device Enrollment Program [DEP])
- Device management
- Application management and deployment in native format
- Continuous OS updates (enforce/defer OS updates)

- Direct inclusion of CMT capabilities or integration with third-party CMTs
- Ability to directly support migration from traditional client management to modern management
- Direct integration with the Microsoft Intune Graph API for app and data protection

2. Provide evidence of a UEM product currently managing at least 10 million devices

3. The product must be available as a SaaS-based deployment regardless of other deployment methods such as on-premises

**Honorable Mentions**

Gartner currently tracks more than 30 vendors in the endpoint management space. While this research identifies eight vendors that have met our inclusion criteria, the exclusion of a vendor does not mean that the vendor and its products lack viability. Below are several noteworthy vendors that did not meet all inclusion criteria but could be appropriate for clients, contingent on requirements:

- **Beijing NationSky Network Technology**: NationSky's NQSky EMM product is a highly used mobility management tool in the Chinese market. Though it met the functionality requirements for managing mobile devices, NationSky lacks sufficient PC management capabilities to satisfy Gartner’s inclusion criteria for UEM.

- **42Gears**: 42Gears UEM provides the base capabilities to manage mobile devices and PCs in addition to its unique ability to manage nontraditional, frontline and IoT devices, such as network printers, point-of-sale and other peripheral devices attached to PCs, mobile devices, or an IoT gateway. Though it met the UEM functionality requirements, 42Gears lacks evidence to support meeting Gartner’s inclusion criterion of managing more than 10 million devices.

- **HCL Software**: Since acquiring BigFix from IBM in 2019, HCL has invested in maintaining BigFix’s robust Windows, macOS, Windows server, Linux and UNIX management and patching capabilities. Its BigFix 10 release added modern OS management, AI-/ML-based intelligence, automation and multicloud support. Though it manages a substantial number of devices and is still used by clients as an all-in-one server and client management and patching tool, HCL BigFix lacks the MDM capabilities required to satisfy Gartner’s inclusion criteria for UEM.
- **Jamf**: Jamf provides robust management capabilities for Apple endpoints and is a featured partner of Microsoft that directly integrates with Endpoint Manager. Clients view Jamf as the premier tool for managing complex or large Apple environments; however, Jamf’s exclusive focus on the Apple ecosystem does not satisfy Gartner’s inclusion criteria for UEM.

- **ManageEngine**: ManageEngine’s Desktop Central UEM Edition extends beyond UEM to include endpoint security, OS and third-party application patching, asset management, IT operations, and IT service management. Though it met the UEM functionality requirements, ManageEngine lacks evidence to support meeting Gartner’s inclusion criteria of a UEM SaaS offering and managing more than 10 million devices.

- **Matrix42**: Matrix42 offers a broader IT management toolset with a strong European presence that combines endpoint management and endpoint security, IT service management, software asset management, and workspace management products. Though it met the UEM functionality requirements, Matrix42 lacks evidence to support meeting Gartner’s inclusion criterion of managing more than 10 million devices.

- **Raynet**: Raynet offers a broad suite of IT management tools that includes endpoint management and security, as well as service and asset management. Though it met the UEM functionality requirements, Raynet lacks evidence to support meeting Gartner’s inclusion criteria of a UEM SaaS offering (due in late 2020) and managing more than 10 million devices.

- **Snow Software**: Snow provides an endpoint management tool offering device management with self-service onboarding/offboarding, hardware life cycle management and software asset management. Though it met most of the UEM functionality requirements, Snow Software lacks evidence to support meeting Gartner’s inclusion criterion of managing more than 10 million devices with UEM capabilities.

- **Tanium**: Building on its depth and expertise in endpoint management, patching, asset management and endpoint security, Tanium continues to evolve into a broader UEM and UES tool. Clients with large, complex, and diverse server and endpoint environments use Tanium as a stand-alone CMT or to complement a UEM tool. Tanium currently lacks the MDM capabilities required to satisfy Gartner’s inclusion criteria for UEM.

- **Virtual Solution**: Virtual Solution offers its SecurePIM mobile containerization solution direct to customers and through partnerships with UEM tools; however, it lacks the broader UEM capabilities to satisfy Gartner’s inclusion criteria for UEM.

**Evaluation Criteria**

**Ability to Execute**

The Ability to Execute criteria evaluate the vendor’s ability to properly resource product development, marketing and sales. Emphasized criteria center on the product itself, but consider the operational support from sales, marketing and R&D, and the vendor’s reputation with customers and performance in the market relative to competitors.
### Table 1. Ability to Execute Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product or Service</td>
<td>High</td>
</tr>
<tr>
<td>Overall Viability</td>
<td>Medium</td>
</tr>
<tr>
<td>Sales Execution/Pricing</td>
<td>Medium</td>
</tr>
<tr>
<td>Market Responsiveness/Record</td>
<td>Medium</td>
</tr>
<tr>
<td>Marketing Execution</td>
<td>Medium</td>
</tr>
<tr>
<td>Customer Experience</td>
<td>Medium</td>
</tr>
<tr>
<td>Operations</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Source: Gartner (August 2020)

### Completeness of Vision

Completeness of Vision focuses on the performance of a vendor’s product as it applies to current market needs, the strategy and performance in delivering to meet that understanding, and the ability of the vendor to innovate for current and emerging needs as well as against its competitors. This metric also assesses a vendor’s geographic strategy and presence, its strategy and roadmap for the product, and its general business model.

### Table 2. Completeness of Vision Evaluation Criteria

<table>
<thead>
<tr>
<th>Evaluation Criteria</th>
<th>Weighting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Understanding</td>
<td>High</td>
</tr>
<tr>
<td>Marketing Strategy</td>
<td>High</td>
</tr>
<tr>
<td>Sales Strategy</td>
<td>Low</td>
</tr>
<tr>
<td>Offering (Product) Strategy</td>
<td>High</td>
</tr>
<tr>
<td>Business Model</td>
<td>Medium</td>
</tr>
<tr>
<td>Vertical/Industry Strategy</td>
<td>Medium</td>
</tr>
<tr>
<td>Innovation</td>
<td>High</td>
</tr>
<tr>
<td>Geographic Strategy</td>
<td>Medium</td>
</tr>
</tbody>
</table>

Source: Gartner (August 2020)
Quadrant Descriptions

Leaders
Leaders are identified as those vendors with strong execution and vision scores and with products that exemplify the suite of functions that assist organizations in managing both their mobile devices and PCs. Leaders also provide guidance and tools to help migrate from traditional client management to modern management, as well as deep integration into endpoint analytics and endpoint security tools to provide a simplified IT administrator and an improved end-user experience.

Challengers
Challengers exhibit a strong set of technologies, marketing and sales execution and intellectual property, as also exhibited by Leaders, but offer solutions in this market tailored to specific market segments or use cases. They may be satisfied with servicing their current customer base or market or lack the strategic support, direction or desire to compete in the Leaders quadrant.

Visionaries
Visionaries exhibit a strong set of capabilities in their current offerings and a complete set of functionalities to address many use cases, although the vendor’s size, the size of its installed base, platform breadth or integration points make it an appropriate choice for some, but not all, buyers.

Niche Players
Niche Players bring specific strengths to this market, including leadership in specific use cases or market segments or verticals. However, their offerings fail to provide a breadth of features that make them relevant to all buyers, regardless of vertical, geographic market or use case.

Context
Several adjustments were made to the UEM market definition and inclusion criteria to increase client value. Adjustments included:

- **Shifting Emphasis:** The elimination of legacy PC operating systems and increased acceptance of remote work has significantly shifted the priority of UEM tools from a focus on mobile devices to a focus on the broader management of both mobile devices and PCs. This includes the ability to remotely deploy and provision devices, applications and updates, and security patches. Less common use cases like IoT, wearables and support for Chrome OS were de-emphasized.

- **Ensuring Comparability:** As complexity and cost reduction initiatives continue to drive client interest in replacing disparate MDM tools and CMTs with UEM, greater focus was placed on
ensuring the comparability of included products. This includes product functionality, geographic coverage, scalability and a common baseline of devices under management.

- **Analytics and Security**: Continued focus on reducing security risk and improving the user experience with technology is driving new capabilities available only when UEM tools are directly integrated with endpoint/workplace analytics, identity and endpoint security tools. In response, inclusion of, or direct integration with, tools that provide this functionality was upgraded from optional to required.

- **Increased Weighting**: Clients view the transition to UEM as a long-term investment, and endpoint management tool migrations are difficult to execute and disruptive to end users. This prompted increased weighting for product marketing strategy and operations to maximize customer awareness and usage of UEM tool capabilities and to ensure that vendors demonstrated ability to scale and sustain operations to meet customer demands.

The end goal of any Magic Quadrant is to provide a level view of comparable products (size, capability and corporate structure) to address the demands of a wide variety of buyers. Not every company’s requirements are identical. We encourage clients to match their functionality, industry expertise, technology and cost requirements to the right vendor, regardless of quadrant.

**Market Overview**

The UEM market continues to evolve since its inception in 2018 as a consolidation of the client management, mobile application management and mobile device management tool markets. Gartner considers UEM as a mature market with limited opportunities for products or vendors beyond new frontline worker technology deployments and increased interest from small and midmarket companies, many of whom were unprepared for the pandemic-induced shift to remote work.

Over the past year, the UEM market was impacted by:

- Near elimination of legacy operating systems (Windows 7) opened the door for co-management and modern management.

- Customer demand for improved security, transparency into endpoint performance, and ability to measure and improve user experience prompted several acquisitions, product announcements, and new functionality delivered by UEM vendors. This has extended the use of telemetry and analytics well beyond providing frictionless, continuous authentication to help inform automation and prioritization of IT admin efforts.

- The pandemic highlighted critical flaws in traditional CMTs as device provisioning, deployment, patching and management failed to scale and support remote clients. Many were ill-prepared to handle the number of devices connected and the volume of data being transmitted over VPN.

- Microsoft 365 customers are being forced to justify the use and incremental cost of additional endpoint management tools because Microsoft Endpoint Manager is included in most entitlements.
Gartner anticipates the future of the UEM market to be shaped by:

- The economic impact of the pandemic.
- The prevalence of remote work as the pandemic wanes or new concerns emerge.
- UEM adoption and embracing integration with analytics, identity and endpoint security tools.
- Adoption of cloud services, SaaS applications and zero trust network access technologies.
- Release of new devices, operating systems, APIs, regulations and management requirements.
- Vendor acquisitions, partnerships and/or product announcements.

Most clients currently use UEM tools predominantly for management of computers or mobile devices; however, Gartner is observing a rapid increase in endpoint management tool consolidation and adoption of co-management for PCs. Clients are also analyzing whether modern OS management is a near-term possibility.

Achieving a single-console approach to endpoint management promises many operational benefits, but Gartner advises organizations to carefully consider the feasibility of this approach based on technical debt, endpoint and infrastructure complexity and diversity, policies and processes, use cases, and application catalog. It is common, and recommended, for an organization to choose a UEM tool that addresses the majority of its requirements, then fill remaining critical gaps with an add-on or another product. Clients should avoid waiting for the perfect tool that addresses all of their requirements as this is rarely found. Waiting often results in increased complexity, administrative overhead and total cost of ownership.

**Gartner Recommended Reading**

*Some documents may not be available as part of your current Gartner subscription.*

- “Critical Capabilities for Unified Endpoint Management Tools”
- “Prepare for Unified Endpoint Management to Displace MDM and CMT”
- “Adopt Continuous Endpoint Engineering and Modern Management to Ensure Digital Workplace Success”
- “Essential Considerations When Choosing Separate PC and Mobile Management Tools”
- “Solution Comparison for Unified Endpoint Management Systems”
- “Hype Cycle for Digital Workplace Infrastructure and Operations, 2020”
- “Mobile OSs and Device Security: A Comparison of Platforms”
- “The Cost Argument for Supporting Android Enterprise Recommended Devices”
“How Markets and Vendors Are Evaluated in Gartner Magic Quadrants”

Note 1 Source of Social Media Analytics Data

- **Approved Methodology:** Gartner conducts social listening analysis leveraging third-party data tools to complement or supplement the other fact bases presented in this research. Due to its qualitative and organic nature, the results should not be used separately from the rest of this research. No conclusions should be drawn from this data alone. Social media data in reference is from 1 July 2017 to 31 March 2020 in all geographies (except China) and recognized languages.

- **Sources Covered:** By default, social media sources considered for analysis include Twitter, Facebook (publicly available information only), aggregator websites, blogs, news, mainstream media, forums and videos (comments only); unless and until specified.

- **The Social Media Analytics Team:** Ritesh Kumar Srivastava and Ayush Saxena from the Social Media Analytics Team contributed to this research.

Social media analytics study results do not represent “global” findings or the market as a whole, but reflect the aggregate crowdsourced opinion of the respondents commenting about the topic on social media.

---

**Evaluation Criteria Definitions**

**Ability to Execute**

- **Product/Service:** Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

- **Overall Viability:** Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization’s portfolio of products.

- **Sales Execution/Pricing:** The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

- **Market Responsiveness/Record:** Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor’s history of responsiveness.

- **Marketing Execution:** The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and
business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

**Customer Experience:** Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

**Operations:** The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

**Completeness of Vision**

**Market Understanding:** Ability of the vendor to understand buyers’ wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

**Marketing Strategy:** A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

**Sales Strategy:** The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

**Offering (Product) Strategy:** The vendor’s approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

**Business Model:** The soundness and logic of the vendor’s underlying business proposition.

**Vertical/Industry Strategy:** The vendor’s strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

**Innovation:** Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

**Geographic Strategy:** The vendor’s strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either
directly or through partners, channels and subsidiaries as appropriate for that geography and market.