Magic Quadrant for Unified Endpoint Management Tools

Published 16 August 2021 - ID G00734620 - 31 min read

By Analyst(s): Dan Wilson, Chris Silva, Tom Cipolla

Initiatives: Digital Workplace Infrastructure and Operations

UEM adoption, vendor acquisitions and partnerships, and incremental product advancements accelerated in 2020. UEM tools are now positioned to help infrastructure and operations leaders enable anywhere operations.

This Magic Quadrant is related to other research:
View All Magic Quadrants and Critical Capabilities

Strategic Planning Assumptions

By 2024, more than half of organizations will consolidate to a unified console for endpoint management and security tasks, which represents a significant increase from fewer than 5% in 2020.

By 2024, endpoint analytics and automation will help digital workplace service staff shift 30% of time spent on endpoint support and repair to continuous engineering.

Market Definition/Description

Gartner defines unified endpoint management (UEM) as a tool that provides agent and agentless management of computers and mobile devices through a single console.

Modern UEM tools:

- Provide a user-centric view of devices across device platforms
- Offer agent and/or agentless management through native Windows 10, macOS and Chrome OS controls
- Offer agentless management through native Apple iOS/iPad OS and Google Android controls
- Aggregate telemetry and signal from identities, apps, connectivity and devices to inform policy and related actions
- Aggregate and analyze technology performance and employee experience data
- Integrate with identity, security and remote-access tools to support zero-trust access and contextual authentication, vulnerability, policy, configuration, and data management
- Manage nontraditional devices, including Internet of Things (IoT) devices, wearables and rugged handhelds
Magic Quadrant

Figure 1: Magic Quadrant for Unified Endpoint Management Tools

Source: Gartner (August 2021)
Vendor Strengths and Cautions

BlackBerry

BlackBerry is a Niche Player in this Magic Quadrant. BlackBerry's UEM product focuses on providing secure access to data, apps and workspaces from mobile devices and PCs. Its operations are geographically diversified, and its clients operate mainly in highly regulated markets in North America and Europe. BlackBerry continues to invest in improvements to its artificial intelligence (AI)-enhanced endpoint security and workspace technology.

Strengths

- **Secure Workspace:** The BlackBerry Digital Workplace combines BlackBerry Access, BlackBerry Dynamics, Cylance endpoint protection technology and Awingu in-browser presentation of virtualized apps and desktops. It provides a secure alternative to deploying endpoints to remote and third-party workers for even the most-security-focused clients. Clients have cited this as a strength in the Gartner Peer Insights reviews and client interaction data, and this has also been echoed in social media discussions about BlackBerry.

- **UEM Plus UES:** BlackBerry offers management and endpoint security elements across its portfolio. Buyers looking for a tightly integrated UEM and endpoint protection toolset, with a single console and the ability to create policies and workflows informed by endpoint security tools, should consider the BlackBerry Spark Suite. It combines entitlements for its UEM and unified endpoint security (UES).

- **Mobility Focus:** BlackBerry's endpoint management strengths and primary use cases remain the ability to securely manage corporate-owned mobile devices and containerization of applications and data for bring your own device (BYOD) use cases, especially for highly regulated or security-centric organizations. Key capabilities that underpin this strength include mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), and identity and access management (IAM).

Cautions

- **Endpoint Diversity:** BlackBerry's UEM provides basic Windows 10, macOS and Chrome OS management; however, it lacks Linux management capabilities. Clients looking to completely migrate away from traditional agent-based management to modern management can use the BlackBerry UEM Migration tool.
Citrix is a Niche Player in this Magic Quadrant. Its Citrix Endpoint Management (CEM) product is focused on providing a digital workspace that includes endpoint management, content collaboration, and virtual applications and desktops. Its operations are geographically diversified, and its clients tend to be 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 managing devices, delivery of virtual applications and desktops, and secure access to applications and data from a single console. This integration is intended to reduce IT administrator overhead and provide a seamless employee experience.
- **Zero Trust**: Citrix Workspace licenses include remote access via Citrix Gateway (NetScaler), the security and experience management-focused Citrix Analytics, and integration with identity and endpoint security tools. Its partnership with Microsoft enables these capabilities to be added to Microsoft’s tooling to enhance the protection of Microsoft 365. Analysis of social media conversations revealed satisfaction with its integrations with Google, Microsoft and OKTA.
- **BYOx**: Zero trust and workspace combine to enable secure access to company resources, as well as containerization capabilities on mobile devices. With this, Citrix provides a secure alternative to deploying endpoints to remote and third-party workers. This includes access to company resources from non-company-owned mobile devices (BYOD) and computers (bring your own PC), even for organizations that operate in highly regulated markets.

**Cautions**

- **Endpoint Analytics**: Although BlackBerry offers strong AI-enabled security analytics, it lacks endpoint analytics capabilities to provide visibility into the performance of devices or applications (unless they are BlackBerry Dynamics wrapped applications) through the lens of employee experience. They also lack remote control support and endpoint automation capabilities to reduce IT administrators overhead.
- **Brand Awareness**: BlackBerry has traditionally struggled to break free from its legacy as a device manufacturer, which has hampered its efforts to break into the pool of traditional UEM buyers. Its brand challenges extend to buyer awareness of its security capabilities.
IBM is a Challenger in this Magic Quadrant. Its IBM Security MaaS360 with Watson product is focused on AI-enhanced UEM and endpoint security. Its operations are geographically diversified, and its clients tend to be midsize enterprises (MSEs) in technology, retail and manufacturing, based in the Americas and Europe. IBM continues to invest in Watson, deeper integration with identity and endpoint security products, and patching capabilities to reduce vulnerabilities.

Strengths

- **Long-Term Strategy:** Citrix’s overall vision and long-term strategy focuses on securing the digital workspace versus securing only the endpoint and complementing its partner Microsoft’s Endpoint Manager for Office 365 application management and modern Windows management.

- **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. Citrix still sells stand-alone CEM licenses if customers are seeking that.

- **Performance:** Customer reviews on Gartner’s Peer Insights platform and feedback collected during client interactions reveals that the most common concern is sluggish performance. This points toward the IT administrator’s use of the CEM console to perform actions and push software to mobile devices, slow Citrix PIM apps performance, and Citrix apps negatively affecting overall device performance.

- **Watson Analytics:** IBM uses Watson to deliver analytics designed to help customers identify, prioritize, triage and resolve security, as well as identity risk or performance and configuration issues on devices managed by MaaS360. Gartner Peer Insights reviews and social media discussions mention efficiencies gained from customizable, automated reporting that helps identify and prioritize critical issues and benchmark configurations against baselines and best practices.

- **Ease of Use:** Clients often reference the catalog of templates and its wizardlike interface as a strength of MaaS360. IBM has also partnered with WalkMe to include its digital adoption platform into the MaaS360 console. This integration helps IT administrators learn and use MaaS360 in the context and flow of work, rather than offline.
Integration: MaaS360 offers more integrations than most of the competition. These include connectors for tools that manage security, vulnerability, identity, IT service and asset, digital adoption, data and analytics, and remote support capabilities. It has also partnered with Microsoft on Conditional Access Device Trust integration and extended MaaS360 integration with its own QRadar, Trusteer and IBM Verify Access for SASE.

Cautions

SaaS Only: Available only as a SaaS solution, MaaS360 does not provide on-premises management options. Despite earning several security certifications (e.g., FedRAMP, SOC II Type 2 and ISO 27000 II), a lack of on-premises hosting may limit MaaS360’s appeal for some users. However, it offers a gateway to enable mobile devices to access email and other applications hosted on-premises.

Corporate Prioritization: MaaS360's positioning in IBM’s security division, along with the company’s decision to use Jamf to manage its own Apple devices, has caused clients to question how strategic MaaS360 is for IBM.

Value Proposition: Although MaaS360 lacks some of the advanced features of its competitors, pricing exceeds that of leading competitors that provide broader endpoint management, security and virtualization capabilities. Capabilities that require additional investment include TeamViewer remote control, which can be purchased from IBM and directly integrated with MaaS360, and third-party virtual private networks (VPNs). Those without a third-party VPN can use MaaS360's mobile VPN, which is available via an add-on for Essentials or Deluxe license bundles, or is included in Premier and Enterprise bundles.

Ivanti

Ivanti is a Visionary in this Magic Quadrant. The Ivanti Unified Endpoint Manager product continues to extend its proven client management capabilities, as it bolsters its modern and mobile device management capabilities with the acquisitions of MobileIron and Pulse Secure. Its operations are geographically diversified, and its clients tend to be enterprise organizations. Ivanti continues to invest beyond UEM capabilities with Neurons to improve its real-time discovery; performance analytics; insights-driven automation and self-healing; patching; zero-trust security; and integration with IT service, asset and cost management tools.

Strengths
Intelligence and Automation: Ivanti Neurons’ intelligence offers active and passive discovery of devices in highly complex, distributed environments. It applies machine learning (ML) to the collected data. This results in derived insights that can inform or be used to automate the remediation of anomalies.

Broad Capabilities: Ivanti offers broad capabilities to manage all Microsoft, Apple and Google OSs; Linux distributions; servers; OEMConfig and Android Open Source Project (AOSP) devices; and wearables. It also can manage devices via SNMP. Ivanti also includes first- (OS) and third-party application patching and integrations with its own and third-party IT asset and service management (ITAM/ITSM) tools. Its acquisition of MobileIron and Pulse Secure in December 2020 closed previous gaps in the management of mobile devices and added security capabilities (mobile threat defense and zero sign-on) and zero trust network access (ZTNA).

Vertical Market Solutions: Ivanti has significantly improved the integration of core products’ endpoint discovery and management capabilities from Ivanti UEM and Ivanti Neurons into existing vertical market solutions — Avalanche and Wavelink. It added new vertical market solutions, such as Ivanti Neurons for Healthcare, which offers improved device discovery, management and patching of medical-use computers, and network-connected medical devices.
ManageEngine

ManageEngine is a Niche Player in this Magic Quadrant. The Desktop Central UEM Edition product continues to add depth to its broad management capabilities. Its operations are geographically dispersed. Its clients tend to be MSEs. ManageEngine continues to invest in adding endpoint detection and response (EDR) to strengthen endpoint security, adding capabilities to its SaaS offering to align with on-premises, and offering remote access and zero-trust capabilities.

**Strengths**

- **Endpoint Diversity:** ManageEngine offers broad capability to manage Microsoft, Apple and Google OSs; Linux distributions (Ubuntu, Red Hat, CentOS, Fedora, Mandriva, Debian, Mint, SUSE, Pardus, Oracle Linux, and derivatives of each); servers; and OEMConfig devices (Samsung, Zebra, Honeywell, Lenovo, Datalogic, Unitech, Nokia, Kyocera, Cipherlab, Seuic and Spectralink).

- **Pricing:** ManageEngine has one of the more affordable UEM offerings in this research, with a list price that begins 20% lower than the next-lowest competitor. Email, phone and chat support are included at no additional cost.

**Documentation:** Ivanti has prioritized the integration of acquired tools, customers and employees, though gaps remain in consolidating customer-facing resources, such as websites and knowledge bases. Migration of documentation, FAQs, quick start guides, reference architecture, etc. from the old websites to Ivanti.com is a work in process. Until the consolidation effort is complete, customers may have difficulty locating training, configuration and architecture reference material, as well as product support information for MobileIron and Pulse Secure environments.

**IT Administrator Experience:** Although the integration of Ivanti, MobileIron and Pulse Secure consoles was delivered rapidly, the IT administrator experience is still fragmented. This becomes more apparent after clicking through the unified console into the underlying technology to perform actions. Gartner predicts that this will improve with each quarterly release; however, clients should be aware of the challenge.

**Legacy:** Although Ivanti has heavily promoted Ivanti Neurons’ value proposition and has fully embraced its “Everywhere Workplace” theme, organizations still require education on what Ivanti is and what happened to MobileIron and LANDesk. Remnants of legacy branding remain in the UEM console, on the Ivanti website and in documentation.
Cautions

- **Licensing Model:** The licensing model is more difficult to understand and administer than those of competitors. Obtaining a quote requires entering the total number of devices to manage, and the technicians that will need to access the system. Both are tiered from 50 to 10,000 devices, and one to 50 additional technicians. They also lack user-based licenses and require additional cost for their Browser Security Plus, Vulnerability Manager Plus, Device Control Plus, Application Control Plus, Analytics Plus and Secure Gateway Server capabilities. These are available a la carte or as part of the Endpoint Security add-on bundle.

- **Consistency:** The on-premises edition of Desktop Central UEM has more-advanced capabilities than its SaaS offering. Desktop Central Cloud UEM does not offer Linux software management, AD reporting or integration with common endpoint security capabilities. Customer reviews on Gartner's Peer Insights platform and feedback collected during client interactions also reveal concerns with the quality and performance of products and support, and the difficulty of on-premises hosted platform upgrades.

- **Remote Access and Zero Trust:** ManageEngine lacks generally available VPN and zero-trust capabilities; however, both are on the 2021 roadmap. Until delivered, third-party solutions are required, which could prove cumbersome for smaller organizations.

Matrix42

Matrix42 is a Niche Player in this Magic Quadrant. The Matrix42 Secure UEM (SUEM) product excels at supporting basic endpoint management and security use cases. Its operations are globally distributed, and clients tend to be MSEs in the Austria, Germany, Switzerland (DACH) region. Matrix42 has completed several recent acquisitions (EgoSecure, FastViewer and Firescope, and a controlling investment in Infowatch Labs), along with investments aimed at enhancing ITAM/ITSM and behavioral dynamic policy enforcement.

Strengths
Extensibility: Matrix 42’s capabilities are well-suited to the endpoint management needs of MSEs. Its first-party (EgoSecure) and partner (Fortinet) security capabilities can integrate with the UEM to automate the detection and remediation of security-related anomalies and malicious activities. The vendor’s third-party application package repository solution (PackageCloud) also integrates with the UEM to automate software packaging and patching. These tools require separate, add-on licensing. Matrix42 also offers its own ITSM platform, which integrates directly with its SUEM offering.

Low-Code Workflow Platform: Its entire workspace platform is built on an extensible, low-code workflow platform that leverages a centralized configuration management database (CMDB) for SUEM and other workloads. This allows customers to tailor the solution for their needs. The Matrix42 Extension Gallery also enables developers to build additional capabilities and integrations with third-party products.

Co-management: Matrix42’s SUEM offers broad endpoint capabilities via an agent and modern management enrollment. This dual or co-management model helps clients migrate from legacy client management to modern management, as they feel comfortable. This transition is assisted by wizards and in-console guides. Matrix42 also offers a product called Enterprise Manager for SCCM, which can be used to extend the capability of Microsoft Configuration Manager.

Cautions

Geographic Focus: Despite its desire to sell globally, Matrix42 lacks strong brand awareness among buyers outside the DACH region, where most of its installed base is. Brand awareness is limited, and growth in other markets has been challenging.

Platform Economics: Matrix42 primarily focuses on selling SUEM and complete digital workspace bundles (plus add-ons). This aligns well with smaller IT organizations that favor complete platforms over point solutions. However, organizations that already have a CMDB, an ITAM/ITSM or endpoint security tools may end up paying extra for capabilities they already have.

Remote Access and Zero Trust: Matrix42 requires third-party tools to complete its zero-trust and remote-access capabilities, lacking an integrated VPN offering at the time of this analysis.
Microsoft

Microsoft is a Leader in this Magic Quadrant. Microsoft Endpoint Manager 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 the IT administrator experience, endpoint analytics and automation, and supporting frontline worker devices and integration with their Azure Virtual Desktop, Windows 365, Defender for Endpoint and Azure Active Directory (AD).

**Strengths**

- **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. Its integration with Azure AD, Defender xDR and Microsoft 365 applications offers improved security and IT administrator experience.

- **Cloud Connected:** Improvements in hybrid Azure AD Join and Tenant Attach have accelerated the adoption of cloud management of devices via co-management and modern management. The ability to migrate when ready is cited during customer reviews on Gartner’s Peer Insights platform, in feedback collected during client interactions, and in social media discussions, as a benefit. This is especially true of organizations that cannot or are not yet ready to exclusively embrace modern management.

- **Product Strategy:** With the growth of Microsoft 365, Endpoint Manager continues to dominate UEM market share. New features and fixes are prioritized based on customer demand, which appears to outpace the availability of development resources. The Endpoint Manager branding has become commonplace among clients, and its popularity on social media has also increased.

**Cautions**

- **Lack of Discovery:** Endpoint Manager depends on local AD or Azure AD to identify devices that should be enrolled and managed. This leaves organizations at risk, because devices on the network are not discoverable without Microsoft Defender for Endpoint or third-party tools.

- **Endpoint Diversity:** Endpoint Manager lacks capabilities to manage Chrome OS and Linux endpoints, as well as some IoT, wearable and rugged frontline devices. As of this writing, Endpoint Manager also lacks a generally available first-party VPN for all endpoints; Tunnel is in preview for iOS, and no date has been provided for Windows.
Complexity: Despite increased investment in Microsoft Learn courses, quick start guides, how-to videos and more-prescriptive guidance, feedback collected during client interactions reveals clients still struggle to keep pace with changes. They also underestimate the overhead required to operate Configuration Manager and integrate it with Intune, Azure AD and on-premises AD. Those that migrated from other client management tools (CMTs) are also frustrated with the lack of third-party application patching capabilities that require a third-party solution. IT leaders are also often confused by inconsistent use of legacy and new branding.

VMware
VMware is a Leader in this Magic Quadrant. Its Workspace ONE product provides improved employee experience through UEM, virtualization, analytics, security, remote access, 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.

Strengths

End-to-End Solution: VMware is the only vendor in this research with a complete package that includes device management (Workspace ONE UEM), single sign-on (SSO; Workspace ONE Access), remote support (Workspace ONE Assist), remote access (Workspace ONE Tunnel and VMware SASE), endpoint security (Carbon Black), analytics and automation (Workspace ONE Intelligence), and virtualization (Horizon). Customer reviews on Gartner’s Peer Insights platform and feedback collected during client interactions reveal satisfaction with Workspace ONE improving the remote worker experience.

Simplicity: VMware Workspace ONE provides several templates, baseline configurations and wizards that help reduce IT administrator overhead. It also seamlessly combines traditional and modern management capabilities, instead of integrating otherwise disparate tools. To simplify the task of keeping pace with changes and updates, VMware’s TechZone website continues to set a high standard for efficiently delivering product information, videos, labs, blogs, implementation guides, learning activity paths, podcasts and reference architecture.
Flexibility: VMware offers the most flexible architecture in this research. Although the competition offers different architectures, they lack the flexibility to choose what components are installed where. With Workspace ONE, clients are not limited to the vendor choosing what workloads can be hosted in SaaS or on-premises. They can architect the solution based on custom needs. Prebuilt connectors enable complex integrations with third-party identity, endpoint security, remote access, IT operations and ITSM tools.

Cautions

Pricing: Clients get the most value from Workspace ONE through advanced features, such as digital employee experience management, risk-based conditional access for zero trust, automation and intelligence. These are only available with the Advanced or Enterprise license tiers, which are priced among the highest in this research.

Windows 10 Management: VMware continues to make investments in modern management of Windows, but adoption has been slower than competitors. Customer reviews on Gartner's Peer Insights platform and feedback collected during client interactions reveal that the most common concern is lack of support for coexistence or co-management with incumbent PC management tools as they understand the transformative nature of a full-scale migration of policies, applications, workflows and devices.

Microsoft 365: VMware customers committed to Microsoft 365 continue to struggle to justify additional investments in a tool seen as overlapping with capabilities they are already entitled to under their existing Microsoft 365 licensing.

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.
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 inclusion or evaluation criteria, or a change in focus by that vendor.

Added
- ManageEngine
- Matrix42

Dropped
- MobileIron
- Sophos

Inclusion Criteria
For Gartner clients, Magic Quadrant research identifies and analyzes the most relevant providers and their products in a market. To qualify for inclusion, vendors must present:

- A generally available, single-license product that demonstrates:
  - Agentless management of Apple iOS, iPadOS and macOS, Google Android, and Windows 10, which includes:
    - Device enrollment and provisioning
    - Device configuration and policy enforcement
    - OS patching and update management
    - Application deployment in native format
  - Agent-based management or prebuilt connectors for CMT integration
  - Direct integration with the Microsoft Intune Graph API for app and data protection
  - Location-agnostic endpoint management (not dependent on LAN/VPN)
Evidence that the UEM product has at least 10 million devices under management, excluding managed devices entitled under trial, freemium or other no-cost use arrangements

A UEM offering as turnkey SaaS (excludes hosted infrastructure as a service [IaaS])

Honorable Mentions

Gartner tracks more than 30 vendors in the endpoint management space. Although 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. Described below are several noteworthy vendors that did not meet all inclusion criteria, but could be appropriate for clients, contingent on requirements:

- **42Gears**: 42Gears UEM provides the base capabilities to manage mobile devices and PCs. This is 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. Although it met the UEM functionality requirements, 42Gears lacks evidence to support meeting Gartner’s inclusion criterion of managing more than 10 million devices.

- **Cisco**: Cisco Meraki Systems Manager offers Cisco-specific integrations, such as automated device enrollment when connected to the network, automated connectivity to Meraki Wi-Fi, integrated VPN connectivity to the Meraki network, remote control to Meraki-connected devices and certificate-based security. Cisco did not meet several of Gartner’s inclusion criteria.

- **FileWave**: FileWave supports management of all Google, Apple and Windows endpoint OSs. As of the March 2021 cutoff date, FileWave did not meet Gartner’s inclusion criteria for agentless management of Windows 10 (released in July 2021).

- **Google**: Google endpoint management is only available as SaaS via Google Cloud Identity and Google Workspace offerings. It offers capabilities to configure macOS and Linux, and manage iOS, iPadOS, Android, Windows and Chrome OS via MDM enrollment. Google did not meet several of Gartner’s inclusion criteria.
**HCL Software**: HCL BigFix offers modern and agent-based management and patching of Windows and macOS, as well as agent-based management and patching of Windows Server, many Linux distributions and UNIX families. As of the March 2021 cutoff date, BigFix did not meet Gartner’s inclusion criteria for MDM (BigFix Mobile was released in July 2021) and turnkey SaaS (which is on its roadmap for 4Q21).

**Hexnode**: The exclusively SaaS-based Hexnode MDM offers capabilities to manage Windows, all Apple OSs, Amazon Fire OS and Android via MDM, but lacks agent-based management. Hexnode did not meet several of Gartner’s inclusion criteria.

**Jamf**: Jamf provides endpoint management and security capabilities for Apple endpoints, with Jamf Pro, Jamf Connect, and Jamf Protect. Its recent acquisition of Wandera expands the Jamf security portfolio to include Threat Defense, web filtering and ZTNA for macOS, iOS, Android and Windows. Jamf’s focus on the Apple ecosystem does not satisfy Gartner’s inclusion criteria for UEM.

**Micro Focus**: Micro Focus ZENworks UEM delivers management of Windows 7, Windows 10, Windows Server, SUSE Linux, Red Hat Linux, and all Apple and Android devices. Micro Focus did not meet Gartner’s inclusion criteria for a turnkey SaaS offering.

**Raynet**: Raynet’s RaySuite UEM solution offers PC management and MDM, inventory, and asset management capabilities that are integrated by a centralized data management technology. Recent UEM development includes an initial SaaS offering of RayManageSoft (RMS) UEM, which is expected to provide feature parity with the RayMobile and RayManageSoft Infinity during the next 12 to 18 months. RaySuite UEM did not meet all of Gartner’s inclusion criteria.

**Sophos**: Sophos offers security-focused UEM capabilities that are tightly integrated into its ecosystem of endpoint, network and cloud security management solutions, appealing primarily to MSEs. Sophos did not meet several of Gartner’s inclusion criteria.

**Tanium**: Tanium continues to expand its endpoint management, patching, asset management and endpoint security capabilities for clients that operate complex server and endpoint environments. Tanium as a Service, its turnkey SaaS offering, was released in mid-2020. As of this writing, Tanium lacks the MDM capabilities required to satisfy Gartner’s inclusion criteria.
Evaluation Criteria

Ability to Execute

The Ability to Execute criteria evaluate the vendor's ability to properly resource product development, marketing and sales. The emphasized criteria center on the product itself, but consider the operational support from sales, marketing and R&D, as well as 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>High</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 2021)

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 vendor's ability 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 2021)

**Quadrant Descriptions**

**Leaders**

Leaders exhibit strong execution and vision scores and exemplify the suite of functions that assist organizations in managing 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 with endpoint analytics and endpoint security tools to provide a simplified IT administrator and an improved employee experience.
Challengers

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

Visionaries

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

Niche Players

Niche Players exhibit leadership in specific use cases, 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

For the 2021 edition of the Magic Quadrant, only minor updates were made to the criteria and ratings. The market definition was updated to add clarity, but no material changes were made. For the inclusion criteria, we clarified requirements for agent-based management or CMT integration, and a turnkey SaaS UEM offering. We also added location-agnostic management capability as a requirement. Finally, sales execution and pricing evaluation criteria weighting was increased from standard to high to reflect heightened cost sensitivity resulting from the pandemic.

The 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 the vendor’s quadrant.
Market Overview

Gartner considers UEM a mature market, with limited opportunities for growth beyond new frontline worker and SMB/MSE use cases. Vendors’ top-line revenue and license growth is driven by organic expansion inside existing customers, such as expansion into management of Windows and macOS devices alongside mobile. Primary client interest drivers are modernization of endpoint management, automation, and improved digital employee experience.

Gartner sees the following forces shaping the UEM market:

- Continued acceptance of remote or hybrid work models in place of exclusively in office work. Gartner’s The Employee Impacts of Anywhere Operations Survey (see Note 2) confirmed that 55% of respondents had trouble patching and managing corporate-owned endpoints, and 48% had problems supporting remote employees. This emphasizes the increased importance of UEM and adjacent tools in enabling anywhere operations.

- Vendor acquisitions, partnerships and product advances are closing the gap between broad-platform and best-of-breed solution offerings.

- Integration with endpoint analytics and endpoint security tools to build proactive and resilient defenses for endpoints under increasing levels of attack.

- A greater focus on insights-driven experience automation (IDEA) requires a centralized platform for collecting and using telemetry to automate fixes to common problems and reduce IT overhead. Gartner’s The Employee Impacts of Anywhere Operations Survey (see Note 2) confirmed that only 24% of respondents are using automation for self-healing. An additional 35% are planning to add this in the next two years.

- Customer demand for fewer tools as manifested by the drive to source UEM and endpoint security tools from incumbent vendors and, increasingly, the same vendor.

Although Gartner continues to see increased adoption of UEM and modern OS management in parallel, we still advise clients to be methodical with the transition from traditional approaches. This is especially so for those with significant technical debt and complexity, and those with more rigid policies and processes.
Clients should avoid waiting for the perfect tool that addresses all of their requirements, because this rarely exists. Waiting often results in increased complexity, administrative overhead and total cost of ownership (TCO). Choose a UEM tool that addresses the majority of requirements, and then address gaps with complementary or supplemental tools.

**Evidence**

Gartner Peer Insights

We considered reviews for Gartner Peer Insights posted from 1 April 2020 through 31 March 2021 for representative vendors in the following markets: CMT, enterprise mobility management (EMM) suites, MAM and UEM.

**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 document. 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 referenced is from 15 May 2019 through 14 May 2021 in all geographies (except China) and recognized languages.

The SMA Team: Fahim Talmeez and Ritesh Srivastava from the Social Media Analytics Team contributed to this research.

**Note 2: The Employee Impacts of Anywhere Operations Survey**

Gartner's The Employee Impacts of Anywhere Operations Survey was conducted online from 4 May through 16 May 2021 to understand the current use and future plans of leaders in workplace infrastructure and operations (I&O).

In total, 109 IT and business leaders participated, coming from a range of regions: North America (47%), EMEA (35%), the Asia/Pacific (APAC) region (9%) and Latin America (8%).

The survey was administered to members of Gartner's Research Circle and was developed collaboratively by a team of Gartner analysts and Gartner's Research Data and Analytics team.

*Note: The results of this study are representative of the respondent base and not necessarily the market as a whole.*
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.

**Document Revision History**

Magic Quadrant for Unified Endpoint Management - 5 January 2021

Magic Quadrant for Unified Endpoint Management Tools - 6 August 2019

Magic Quadrant for Unified Endpoint Management Tools - 23 July 2018
Recommended by the Authors

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

Embrace Windows 10 Modern Management to Enable a Highly Distributed Digital Workplace

2020 Strategic Roadmap for Digital Workplace Infrastructure and Operations

Predicts 2021: Digital Workplace Infrastructure and Operations

How Markets and Vendors Are Evaluated in Gartner Magic Quadrants
### 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>High</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 2021)
### 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 2021)