Magic Quadrant for Endpoint Management Tools

5 January 2026 - ID G00825650 - 53 min read

By Tom Cipolla, Lina Al Dana, **and 4 more**

Endpoint management tools are essential for managing, securing and enabling employee computing devices. I&O leaders should use this research to guide investment in these tools.

Strategic Planning Assumption

By 2029, over 50% of organizations will adopt autonomous endpoint management (AEM) capabilities within advanced endpoint management and digital employee experience (DEX) tools, an increase from 15% in 2026.

Market Definition/Description

This document was revised on 5 January 2026. The document you are viewing is the corrected version. For more information, see the **Corrections** *page on gartner.com.*

Gartner defines an endpoint management tool as a platform or tool that provides configuration management, patching and deployment of operating systems and applications for computers or mobile devices.

Endpoint management tools are used to provide management capabilities for endpoint devices of various operating systems. These tools help maintain cybersecurity hygiene and enable end-user computing operations and automation by facilitating operating system and application deployment, patching and configuration management.

Mandatory Features

- Agent-based or agentless management for any of these operating systems:

  - Apple iOS and iPadOS

  - Apple macOS

  - Google Android

  - Microsoft Windows (endpoint versions)

- Support the following core features for the specified operating system:

  - Application deployment

  - Device configuration and policy enforcement through a graphical user interface with predefined selectable options

  - Device enrollment and provisioning

  - OS patching and update management

- Product must be able to operate as a turnkey SaaS (vendor hosted and operated, not infrastructure as a service [IaaS] and not entirely on-premises).

- Role-based access control (RBAC) to support geographic or line of business (LOB) device population administrative permissions (dedicated support teams for a portion of the population).

Common Features

- Support for autonomous endpoint management (AEM) through the inclusion of digital employee experience (DEX) measurements to measure patch success, configurable patching rings and customizable patch automation based on confidence (success) levels.

- Agent or agentless management, including device discovery, inventory, configuration, OS updates and patching, policy management, encryption management and software deployment of:

  - Google ChromeOS

  - Internet of Things (IoT) devices

- Ruggedized device management (Android OEMConfig or Android Open Source Project)

- Linux, including any of the following: Debian, Red Hat Enterprise Linux, SUSE and Ubuntu

- Wearable device management (e.g., augmented reality/virtual reality [AR/VR] headsets, wrist-worn devices)

- Third-party application patch automation, including a third-party application package repository.

- Support for the full spectrum of mobile management, including mobile device management (MDM), supervision (iOS) and fully managed (Android) and mobile application management (MAM).

- Containerized mobile applications to protect corporate data, such as prevention of copy/paste, attachment saving and printing to nonapproved destinations.

- Ability to erase corporate data from devices upon employee separation without having physical device access.

- Capability for device imaging and reimaging.

- Enterprise app store for employee self-service.

- Agent-based management or prebuilt connector for client management tool (CMT) integration.

- Customizable reporting and dashboarding capabilities.

- Support for modern automatic enrollment and provisioning methods, including:

  - Microsoft Windows Autopilot

  - Apple Business Manager

  - Android zero-touch enrollment, which requires Android Enterprise

  - Other similar automatic enrollment and provisioning supported by device manufacturers or operating system vendors

- Configuration of PC and mobile devices for limited use by frontline or task workers or to be used as kiosks, digital signage, utility and/or a shared device.

- Extended features and integrations:

  - Vulnerability assessment and prioritization, either via native features within the tool or via integration with external tools

  - IT service management (ITSM) and configuration management database (CMDB) integration

  - Multitenant support

Magic Quadrant

Figure 1: Magic Quadrant for Endpoint Management Tools

As of December 2025   © Gartner, Inc
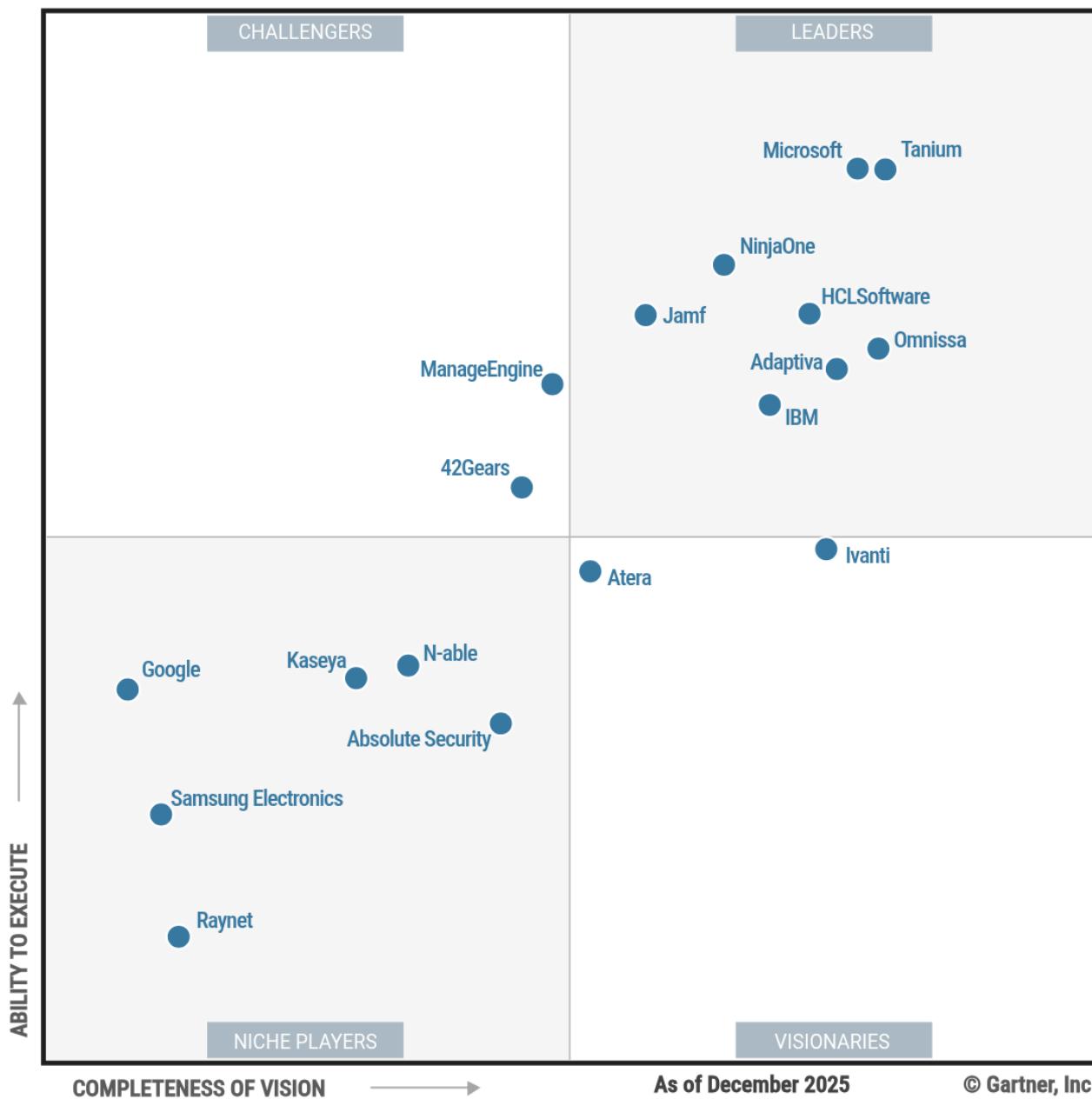
Gartner

Vendor Strengths and Cautions

42Gears

42Gears is a Challenger in this Magic Quadrant. Founded in 2009, it is a privately held company headquartered in Bangalore, India, with operations located in the United Kingdom and North America. Its endpoint management tool, SureMDM, supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS, and Linux devices.

The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises and turnkey SaaS, with geographical hosting available

in AWS and Google Cloud Platform (GCP) regions across the United States, Europe, the Middle East and APAC.

SureMDM is licensed per device, with available tiers including Standard, Premium and Enterprise.

Strengths

- **Market understanding:** 42Gears primarily targets SMB and midmarket segments, but has scaled to serve enterprises of all sizes. Customers benefit from flexible hosting, installation options and deep integration with enterprise security tools.

- **Customer experience:** Peer Insights feedback and client interactions indicate generally high satisfaction. Dedicated customer success managers help customers gain value quickly.

- **Product:** SureMDM supports a broad range of operating systems and device types. The platform is especially strong for managing mobile, ruggedized and specialty devices used in retail and frontline environments where kiosks and shared devices are utilized.

Cautions

- **Sales strategy:** 42Gears does not adapt its sales strategy by customer persona or geography, which may limit effectiveness across regions and roles.

- **Marketing execution:** Despite active social marketing efforts, Gartner client awareness of 42Gears remains low, which may limit growth.

- **Market responsiveness:** 42Gears relies on a small number of formal feedback channels that are limited in effectiveness. This can delay product improvements, cause misaligned priorities and reduce alignment with evolving customer needs.

Absolute Security

Absolute Security is a Niche Player in this Magic Quadrant. Founded in 1993, it is a privately held company headquartered in Seattle, Washington, U.S., with operations primarily in North America. Absolute Security acquired Syxsense in September 2024, adding endpoint management to its portfolio.

Its endpoint management tool, Absolute Secure Endpoint Resilience for Automation, supports Windows, macOS, Linux and ChromeOS (additional license required). The platform

offers a repository of prepackaged applications for simplified deployment. It is hosted via turnkey SaaS with geographical hosting options available in all Azure regions. The solution is FedRAMP (Moderate) authorized. Licensing is per device, with special pricing available for education and government customers.

Strengths

- **Innovation:** Absolute Security holds over 206 patents for endpoint management and security, including its firmware-embedded Absolute Persistence technology that enables BIOS-level PC and OS recovery. The platform provides low-code automation and AI-driven remediation to identify and resolve vulnerabilities, leveraging GenAI to summarize threat intelligence and suggest remediation steps.

- **Vertical/industry strategy:** Absolute Security tailors its platform to verticals like finance, healthcare, government and retail, offering compliance dashboards, HIPAA controls, offline patching and automation. This focus helps ensure security and operational resilience in regulated and distributed IT environments.

- **Product strategy:** Absolute Security publishes a public roadmap with quarterly releases shaped by customer input and strategic themes, including AI, automation, and compliance. This approach keeps product development aligned with customer needs and evolving industry trends.

Cautions

- **Mobile device management:** Absolute Security does not support mobile device management for Android, iOS or specialty devices. These limitations reduce its suitability for organizations with diverse device ecosystems or mobile-first environments.

- **Market responsiveness:** Absolute Security's value proposition is heavily oriented toward security buyers and their use cases. This focus can limit sales effectiveness with end-user services or digital workplace buyers who prioritize operations and employee experience alongside security.

- **Marketing execution:** Absolute Security is best known for device control and BIOS-level security rather than endpoint management capabilities. Low customer awareness may limit growth.

Adaptiva

Adaptiva is a Leader in this Magic Quadrant. Founded in 2004, it is a privately held company headquartered in Kirkland, Washington, U.S., with operations distributed throughout North America, Europe and APAC.

Its endpoint management tool, OneSite, supports Windows, macOS (limited) and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises and turnkey SaaS, with geographical hosting available in the United States, the United Kingdom, Germany, Japan, Singapore and Australia.

OneSite is licensed per device, with license options including OneSite Patch, OneSite Anywhere and OneSite Health.

Strengths

- **Market understanding:** Adaptiva's strategy focuses on enabling large-scale, low-touch endpoint management through peer-to-peer delivery, real-time control and integration with enterprise tools. By reducing operational labor through intelligent automation, customers can streamline endpoint management and allocate resources to higher-value IT initiatives.

- **Innovation:** Adaptiva supports autonomous, scalable endpoint management with real-time visibility and integration across platforms and third-party tools, and has strategic partnerships with Tenable, SentinelOne, CrowdStrike and Microsoft. This helps IT and security teams reduce manual effort, accelerate remediation and maintain compliance across large enterprise environments.

- **Product strategy:** Adaptiva's roadmap is shaped by customer and partner input, prioritizing scalable automation, granular controls, and real-time AI insights.

Cautions

- **Marketing:** Adaptiva utilizes fewer marketing channels and produces less content than other vendors in this market. While customer awareness of its Microsoft companion product is high, Gartner clients report a lack of awareness of its stand-alone endpoint management product, which may limit growth.

- **Product:** Adaptiva does not support modern device management (MDM) via enrollment without an on-device client for any platform and does not support mobile device management for Android or iOS. These limitations reduce its suitability for organizations with diverse device ecosystems or mobile-first environments.

- **Sales strategy:** Adaptiva has begun transitioning from a direct-only model to a channel-first strategy leveraging OEMs, resellers and co-selling partnerships with security vendors. Although Adaptiva is making progress in this transition, its historical reliance on direct sales can limit short-term growth.

Atera

Atera is a Visionary in this Magic Quadrant. Founded in 2011, it is a privately held company headquartered in Tel Aviv, Israel, with operations distributed throughout the Middle East, North America and Europe.

Its endpoint management tool, Atera, supports Windows, macOS and Linux device management, and includes a repository of prepackaged applications for simplified deployment. The platform is hosted via turnkey SaaS, with geographical hosting options that include Azure regions within North America and Europe.

Atera uses a per-technician licensing model, with options including Professional, Expert, Master and Enterprise tiers, as well as special pricing models for managed service providers (MSPs).

Strengths

- **Market understanding:** Atera utilizes a structured feedback loop to remain aligned with current and future market demands. Its vision centers on evolving endpoint management from traditional tools into autonomous, AI-driven workflows that reduce manual effort and support faster, more scalable IT operations.

- **Innovation:** Atera heavily utilizes AI, machine learning, GenAI and agentic AI within its base platform and its AI Copilot and IT Autopilot tools to automate endpoint tasks, enable natural language interaction, and support intelligent, autonomous issue resolution. This establishes a future-ready platform for increased autonomous operations.

- **Business model:** Atera's per-technician licensing model allows unlimited endpoint management for a flat monthly or annual fee per technician. This unique approach applies to both IT departments and MSPs, offering a predictable cost model for growing enterprises and MSPs.

Cautions

- **Operations:** Atera has a limited global operations capability. Though it offers 24/7 support, customers with dispersed geographic operations should evaluate whether Atera can effectively service them in their country.

- **Scalability:** Atera is smaller than most vendors in this report, which may cause concern among larger enterprises about the company's ability to scale to accommodate their needs if it experiences rapid growth.

- **Product:** Atera does not support modern device management via enrollment without an on-device client for any platform and does not support mobile device management for Android or iOS. These limitations reduce its suitability for organizations with diverse device ecosystems or mobile-first environments.

Google

Google is a Niche Player in this Magic Quadrant. Founded in 1998, it is a publicly held company headquartered in Mountain View, California, U.S., with geographically diversified operations.

Its endpoint management tool, Google Endpoint Management, supports Windows, macOS, iOS/iPadOS, Android Enterprise, ChromeOS and Linux. The platform does not offer a repository of prepackaged applications. It is hosted via turnkey SaaS within any supported Google Workspace region and holds FedRAMP (High) authorization.

Licensing for Google Endpoint Management is tied to a Google Workspace or Cloud Identity subscription, with features varying by Workspace edition, such as Business Starter, Business Standard, Business Plus and Enterprise.

Strengths

- **Geographic strategy:** Google has globally distributed operations and can accommodate customers of all sizes and complexity. Google Workspace is hosted on Google's global network of data centers, which enables customers to comply with data sovereignty requirements.

- **Overall viability:** Google consistently demonstrates strong financial viability, high profit margins and consistent growth across its core segments. This reduces risk for customers and partners relying on its ecosystem.

- **Pricing model:** Google Endpoint Management uses a per-user licensing model bundled with Workspace and Cloud Identity tiers at no additional charge. This provides existing Google Workspace customers with a cost-efficient capability.

Cautions

- **Marketing strategy and execution:** Google's endpoint-management-specific marketing is limited. While customer awareness of the overall Google Workspace platform is high, Gartner client awareness of Google's endpoint management capabilities is low, which may impact adoption.

- **Product:** Except for ChromeOS device management, Google Endpoint Management's capabilities are limited and basic compared with those of other vendors in the Magic Quadrant. Google also does not publish a feature roadmap for customers. Prospective buyers should evaluate the offering thoroughly to determine if its capabilities will meet their current and future needs.

- **Innovation:** Google Endpoint Management's capabilities are basic and foundational, with limited usage of advanced technologies such as AI, GenAI and agentic AI.

Google declined requests for supplemental information. Gartner's analysis is therefore based on other credible sources.

HCLSoftware

HCLSoftware is a Leader in this Magic Quadrant. It is the software division of HCLTech and headquartered in Noida, India. No geographic data related to operations was supplied.

Its endpoint management tool, HCL BigFix Workspace+, supports Windows, macOS, iOS/iPadOS, Android Enterprise and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises, fully managed hosted instance and turnkey SaaS, with geographical hosting options in the United States, the Netherlands, Singapore and India.

HCLSoftware BigFix Workspace+ is licensed on a per-user or per-device basis.

Strengths

- **Overall viability:** HCLSoftware consistently demonstrates strong financial viability, high profit margins and consistent growth across core segments. This reduces risk for

customers and partners relying on its ecosystem.

- **Integration and partnerships:** HCL BigFix Workspace+ integrates with a large number of advanced security, IT operations and identity management tools. Strategic partnerships with Tenable, Qualys, Rapid7, ServiceNow, AWS and Azure further enhance its innovation ecosystem. Enterprise customers benefit from these extensive integrations and partnerships.

- **Sales strategy:** HCLSoftware utilizes a large number of sales channels, including resellers, MSPs and an ecosystem of more than 2,000 partners in 129 countries. This provides flexibility in contracting and enables customers to choose their preferred reseller.

Cautions

- **Product:** The turnkey SaaS version of HCL Bigfix Workspace+ is limited compared to the on-premises or managed hosted instance. Some advanced features or modules available in legacy BigFix may not yet be fully supported or configurable in the SaaS version. Customers should assess whether BigFix SaaS aligns with their needs, especially in highly regulated or complex IT environments.

- **Business model:** HCLSoftware is carefully and slowly shifting toward outcome-based service models that blend software and services into "service as software" offerings powered by BigFix automation. While HCLSoftware has no current plans to replace or eliminate the existing licensing model, pricing models and bundling may eventually change. Customers should work closely with their account teams to fully understand the potential benefits and impacts of this model.

- **Customer experience:** Feedback via Gartner Peer Insights and client interactions reveals mixed satisfaction with HCL BigFix Workspace+. The most common negative items include the user interface and a complex setup.

IBM

IBM is a Leader in this Magic Quadrant. Founded in 1911, it is a publicly held company headquartered in Armonk, New York, U.S., with geographically diversified operations.

Its endpoint management tool, IBM MaaS360, supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS, and has partial support for Linux. MaaS360 offers a repository of pre-packaged applications for simplified deployment. Geographical hosting options include Europe (Germany and France), the United States and

APAC. Customers may also use a private cloud deployment in any AWS region. The solution is FedRAMP (Moderate) authorized.

MaaS360 is licensed per user and per device, with available tiers including Essentials, Deluxe, Premier and Enterprise.

Strengths

- **Operations:** IBM has operational staff located in almost every region of the world and differentiates its go-to-market strategies for each geography. It offers flexible hosting options with global coverage and FedRAMP Moderate authorization, enabling customers from nearly all geographies to comply with data sovereignty and high security requirements.

- **Product:** MaaS360 provides an extensive number of features that enable autonomous operations, including mobile threat defense, user risk scoring, and automated compliance enforcement for proactive and adaptive endpoint protection.

- **Innovation:** MaaS360 leverages machine learning and GenAI to deliver real-time threat detection and policy recommendations, as well as natural language support to accelerate endpoint operations. IBM MaaS360 Advisor provides tailored security and productivity insights, detects anomalies, suggests policy changes, and generates predictive analytics to improve endpoint management.

Cautions

- **Business model:** MaaS360 represents a small part of IBM's overall portfolio. IBM is strategically focused on hybrid cloud and AI, which could limit its focus on endpoint management.

- **Sales strategy:** MaaS360's list price is on the higher end among vendors in this Magic Quadrant. Additionally, IBM does not tailor its sales strategy to match ideal customer personas. Higher prices, combined with a lack of a focused sales strategy, will inhibit its ability to sell the product.

- **Marketing strategy:** Gartner clients report a lack of awareness of IBM's overall endpoint management capabilities outside of mobile device management, which can limit growth.

Ivanti

Ivanti is a Visionary in this Magic Quadrant. Founded in 1985, it is a privately held company headquartered in South Jordan, Utah, U.S., with operations diversified across North America, Europe and APAC.

Its endpoint management tool, Ivanti Neurons for Unified Endpoint Management (UEM), supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS, and Linux. The platform offers a repository of prepackaged applications for simplified deployment (additional license required). Hosting options include on-premises (with the legacy Ivanti Endpoint Manager) and turnkey SaaS, with geographical hosting available in Azure regions worldwide. It is FedRAMP (Moderate) authorized.

Neurons for UEM is licensed per user and per device, with available tiers including Secure UEM Professional, Secure UEM Professional Plus and Secure UEM Premium.

Strengths

- **Geographic strategy:** Ivanti offers extensive geographical hosting capabilities, with options available in every region of the world, and maintains sales, marketing and operational staff in almost all regions. Customers benefit from faster service delivery, localized support and compliance with regional data regulations.

- **Sales strategy:** Ivanti employs a balanced, multichannel sales strategy and extends discounting flexibility to its extensive partner network. Neurons for UEM's list price is just below average and represents value for the breadth of included capabilities.

- **Product:** Ivanti Neurons for UEM is a broad and deep platform focused on managing almost all platforms and operating systems. It features tools to improve digital employee experience, autonomous endpoint management and risk-based vulnerability management. Ivanti uses AI and machine learning for anomaly detection and performance monitoring, and offers native remote control across all major platforms except Linux and ChromeOS.

Cautions

- **Vendor delivery and execution:** Updates to Ivanti Neurons for UEM are delivered via a quarterly release cadence, with minor releases as needed. From July 2024 to July 2025, it has had four quarterly and four minor releases. Slower release cadences can delay access to critical features and could result in slower responses to emerging threats and reduced agility in adapting to enterprise needs.

- **Operations:** Ivanti has experienced a number of exploitable vulnerabilities in its legacy Endpoint Manager product over the past 12 months. Ivanti is committed to transparency through its published vulnerability disclosure policy, but unpatched vulnerabilities increase customer risk and can erode confidence in the vendor's products.

- **Customer experience:** Analysis of Gartner Peer Insights and other external customer experience measurements indicates general dissatisfaction with Ivanti. Gartner clients often express frustration about historical security incidents within Ivanti's other products and concerns about overall support quality.

Jamf

Jamf is a Leader in this Magic Quadrant. Founded in 2002, it is a publicly held company headquartered in Minneapolis, Minnesota, U.S., with operations primarily based in North America, Europe, APAC and the Middle East.

Its endpoint management tool supports macOS, iOS/iPadOS and Android (Enterprise and OEMConfig). The platform offers a repository of prepackaged macOS applications for simplified deployment. Hosting options include on-premises and turnkey SaaS, with geographical hosting in the United States, Germany, Australia, Japan and the United Kingdom.

Jamf is licensed per device, with available tiers including Jamf for Mac, Jamf for Mobile, Jamf Now for Small Business and Jamf for K-12.

Strengths

- **Market responsiveness:** Jamf is recognized as an Apple device management leader with strong client loyalty. Clients frequently acknowledge Jamf as a critical component of their Apple device management strategy. To provide a full cross-platform mobile management capability, Jamf recently added Android device management to its product portfolio.

- **Product:** Jamf is widely regarded as the gold standard for Apple device management, especially in enterprise and education environments. The platform supports deep macOS configuration options, including granular control over system preferences, security settings and native Apple features.

- **Marketing execution:** Jamf hosts a number of in-person and online events for customers and prospects and is well known as an Apple-centric device management platform. Its

marketing efforts feature engaging and thought-leading content delivered through multiple channels.

- **Product strategy:** Jamf recently added Android device management to its portfolio in response to customer and market demand. While this change recognizes that typical organizations require more than Apple OS support, Jamf has historically chosen not to support other platforms, which has limited its growth potential.

- **Operations:** As of 2Q25, Jamf is not profitable on a generally accepted accounting principles (GAAP) basis. The company reported a net loss of $20.9 million in its quarterly filing. This may result in disruptions to operations, support or other back-office functions, if significant changes are not made to achieve profitability.

- **Business model:** Historically focused on Apple-only endpoint management, Jamf's future revenue is heavily dependent on Apple's ecosystem and policies. The addition of Android support helps diversify its business model, but overreliance on Apple, with only 9.2% of the enterprise PC market share, can limit growth potential.

Kaseya

Kaseya is a Niche Player in this Magic Quadrant. Founded in 2000, it is a privately held company headquartered in Miami, Florida, U.S., with operations in North America, Europe and APAC.

Its endpoint management tool, Datto RMM, supports Windows, macOS and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include turnkey SaaS, with geographical hosting in the United States, Germany, Ireland and Australia.

Datto RMM is licensed on a per-device basis, with plans available for MSPs and enterprise customers.

Strengths

- **Product strategy:** The majority of Kaseya's customers are MSPs. Datto RMM is a modern remote monitoring and management (RMM) tool built to scale MSP operations. Agent-based monitoring provides real-time visibility into device health and performance across

customer networks, which enables rapid deployment of changes across multiple customer environments.

- **Overall viability:** Kaseya continues to grow year over year and is profitable, with a large portfolio of customers in all industries. Its MSP customer base provides a consistent recurring revenue stream, resulting in financial stability.

- **Extensibility:** Datto RMM supports over 200 third-party integrations, including deep integration with Microsoft 365, antivirus, backup, security tools and IT service management (ITSM) platforms. Customers can easily integrate Datto RMM with their best-of-breed tools.

Cautions

- **Customer experience:** Analysis of Gartner Peer Insights and other external customer experience measurements indicates mixed opinions on Kaseya's business practices. Customers cite concerns regarding customer support and responsiveness, along with a lack of support for mobile device management.

- **Product:** Datto RMM is built for MSPs to manage multiple customer environments with minimal labor. However, enterprise customers may find it challenging to use, and its lack of support for mobile device management may require customers to purchase an additional tool.

- **Vertical/industry strategy:** Kaseya does not demonstrate significant corporate investment or targeted marketing efforts aimed at specific verticals. Lack of vertical specialization can result in feature gaps in regulated or high-security industries such as healthcare, financial services and local and federal government.

ManageEngine

ManageEngine is a Challenger in this Magic Quadrant. Founded in 2002, it is a division of Zoho Corporation, a privately held company headquartered in Del Valle, Texas, U.S., with globally distributed operations.

Its endpoint management tool, ManageEngine Endpoint Central, supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS, and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises, customer cloud hosting (AWS, Azure, GCP) and turnkey SaaS.

Vendor-provided geographic hosting options are available in North America, China, the Middle East, Europe and APAC.

Endpoint Central is licensed per device. Available tiers include Professional, Enterprise, UEM and Security.

Strengths

- **Overall viability:** ManageEngine has grown significantly in the past three years and is profitable. To accommodate this growth, it has increased the number of employees, reducing risk for customers relying on its ecosystem.

- **Operations:** The company has operational staff established in 12 countries and offers flexible hosting options with extensive global coverage. This enables customers from all geographies to comply with data sovereignty requirements.

- **Product strategy:** Endpoint Central supports a wide variety of device types and operating systems. It provides deep automation and scripting capabilities, a comprehensive extension library, risk-based vulnerability prioritization, and autonomous patching.

Cautions

- **Vendor delivery and execution:** Updates to Endpoint Central are delivered via a monthly release cadence. Most updates over the past year were fairly minor. Slower major feature release cadences can delay access to critical features, potentially leading to reduced agility in adapting to enterprise needs. ManageEngine has recently implemented an extensible framework designed to significantly enhance the platform's rapid release capabilities.

- **Innovation:** While Endpoint Central leverages machine learning techniques for vulnerability prioritization and patching, it has limited usage of newer technologies such as GenAI. Its AI-powered assistant, Ask Zia, is integrated into Endpoint Central for reporting, remote support and management automation, but broader AI adoption is limited.

- **Marketing execution:** While ManageEngine produces a large quantity of marketing materials, content specific to Endpoint Central is lower in both quantity and quality. Ineffective or lower-quality marketing content limits the vendor's ability to attract new customers.

Microsoft

Microsoft is a Leader in this Magic Quadrant. Founded in 1975, it is a publicly held company headquartered in Redmond, Washington, U.S., with globally diversified operations.

Its endpoint management tool, Microsoft Intune, supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS, and Linux. Intune offers a repository of prepackaged Windows applications for simplified deployment (additional license required). Hosting options include turnkey SaaS (available in any Azure location) for Intune. On-premises and hybrid options for managing Windows 11 and servers are available with Microsoft Configuration Manager. Intune holds FedRAMP (High) certification.

Intune Plan 1 licensing is included with Microsoft 365 Business Premium and A3/G3/E3 and higher bundles with additional capabilities, and can be purchased separately through Microsoft's Enterprise Mobility + Security (EMS) bundles and stand-alone Intune SKUs. On 4 December 2025, Microsoft announced that select Intune Suite capabilities will be included in Microsoft 365 E3 and Microsoft 365 E5 subscription plans in the coming months.

Strengths

- **Marketing execution:** Microsoft Intune is the default choice for many Microsoft customers, and product awareness is very high. Microsoft effectively leverages a wide variety of channels to convey its messaging, including the Microsoft Security and Microsoft Mechanics series with hundreds of videos containing prescriptive instructions and thought-leading content.

- **Operations:** Microsoft's scalability is extensive. With globally distributed staff, the company effectively delivers across diverse industries and geographies.

- **Geographic strategy:** Microsoft offers local hosting support in nearly every geographic region. It holds a vast number of relevant cyber and operational certifications, and enables customers to benefit from faster service delivery, localized support, and compliance with regional data regulations.

Cautions

- **Sales strategy:** Microsoft does not adapt its Intune sales strategy to vertical or geographic customer personas. Most customers receive Intune as part of their Microsoft 365 license bundles, and this one-size-fits-all approach can diminish the perceived value of Intune.

- **Product:** Gartner clients frequently report unpredictable latency within the product. This latency often results in delayed reporting, policy synchronization, and application deployments, which hamper endpoint management effectiveness for critical activities.

- **Customer experience:** Analysis of Gartner Peer Insights and similar sources indicates a prolonged general dissatisfaction with Intune's steep learning curve, reliability and troubleshooting challenges, along with limited reporting and status visibility.

N-able

N-able is a Niche Player in this Magic Quadrant. Founded in 2000, it is a publicly held company headquartered in Burlington, Massachusetts, U.S., with operations distributed throughout North America, Europe and APAC.

Its endpoint management tool, N-able N-central, supports Windows, macOS, iOS/iPadOS and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises and turnkey SaaS, with geographical hosting available in almost every country worldwide.

N-able N-central is licensed on a per-device basis, with available tiers including Essential and Professional.

Strengths

- **Overall viability:** N-able's customer base consists of over 25,000 MSPs and small to midmarket businesses globally, and the company has demonstrated solid year-over-year growth and has a steadily growing employee base, which reduces risk for customers relying on its ecosystem.

- **Innovation:** N-able uses AI for monitoring, threat detection, forecasting and autonomous remediation. It leverages private AWS-hosted models, agentic AI frameworks, and generative scripting, enabling faster issue resolution, improved operational efficiency and enhanced service quality through intelligent automation, multilingual support, and proactive endpoint monitoring.

- **Market understanding:** N-able is focused on MSPs and small to midmarket businesses, and understands the unique challenges its customers face. Its roadmap is focused on its customers' needs, and its value proposition resonates with them..

Cautions

- **Sales strategy:** Due to its heavy focus on MSPs, N-able differentiates its sales strategy for enterprise customers by geography and customer size, but not by vertical or role. This limited differentiated approach could hamper enterprise engagement and limit relevance across verticals, and could reduce effectiveness in addressing specific role-based needs and buying behaviors.

- **Marketing execution:** While N-able is well known among the MSP community, Gartner enterprise clients report a lack of awareness of its overall endpoint management capabilities, which may limit growth.

- **Customer experience:** N-able features only a few reference accounts on its website and has a limited number of published case studies. This can signal limited proof of success, making it harder to evaluate real-world impact or justify investment.

NinjaOne

NinjaOne is a Leader in this Magic Quadrant. Founded in 2013, it is a privately held company headquartered in Austin, Texas, U.S., with operations distributed throughout North America, Europe and APAC.

Its endpoint management tool, NinjaOne Endpoint Management, supports Windows, macOS, iOS/iPadOS, Android (Enterprise and OEMConfig), and Linux. The platform offers a repository of prepackaged applications for simplified deployment. It is hosted via turnkey SaaS, with geographical hosting options in AWS regions within North America, Europe and APAC. NinjaOne Endpoint Management holds FedRAMP (Moderate) certification.

Licensing is per device via 11 tiers, including Advanced, Enterprise and Mobile Device Management capabilities. A Pro tier at each level includes remote control functionality.

Strengths

- **Customer experience:** NinjaOne delivers a strong customer experience through dedicated customer success managers focused on value over sales, proactive account health tracking, and self-service resources such as certifications and technical documentation. Analysis of Gartner Peer Insights and other external customer experience measurements reflects generally positive customer sentiment, especially with ease of use and time to value.

- **Sales execution/pricing:** NinjaOne pricing is at the lower end of vendors in this Magic Quadrant. Core bundles tailored to the unique needs of enterprise IT buyers and MSPs

help customers to achieve a modern, cost-effective solution.

- **Overall viability:** Ninja has experienced significant growth in customers over the last three years and has increased its operational capability by sustainably growing its employee base. In February 2025, NinjaOne raised $500 million in Series C extensions led by ICONIQ Growth and CapitalG, reaching a $5 billion valuation to fuel innovation and expansion.

Cautions

- **AI adoption:** NinjaOne currently has limited usage of newer technologies such as GenAI. While several items are on the roadmap, the current lack of rapid innovation fueled by advanced technologies could limit long-term competitiveness against emerging AI-powered platforms.

- **Customer awareness:** While overall customer awareness of NinjaOne has recently increased, many Gartner clients remain unaware of its overall endpoint management capabilities. Increased customer awareness will enhance prospects' ability to find the vendor and could drive growth.

- **Business model:** NinjaOne's historical focus has been MSPs, small-to-medium businesses and small enterprises. To satisfy growing demand from larger enterprise segments, the company is evolving its platform, integrations and channel strategy. However, the effectiveness of these efforts at scale remains to be demonstrated.

Omnissa

Omnissa is a Leader in this Magic Quadrant. Founded in 2024, it is a privately held company headquartered in Mountain View, California, U.S., with globally distributed operations.

Its endpoint management tool, Omnissa Workspace ONE UEM, supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS, and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises (by exception only) and turnkey SaaS, with geographical hosting available in North America, the United Kingdom, Europe and APAC. FedRAMP certification is in progress as of the publication date of this Magic Quadrant.

Workspace ONE UEM is licensed per device or per user, with available tiers including Enterprise Edition, UEM Essentials, Desktop Essentials and Mobile Essentials, along with options for frontline and education use cases.

Strengths

- **Product:** Omnissa Workspace ONE UEM is a mature, AI-driven solution offering deep automation and comprehensive endpoint management capabilities across all major operating systems. Customers benefit from intelligent, scalable endpoint management with proactive remediation, streamlined operations and continuous alignment to desired-state configurations.

- **Vertical/industry strategy:** Workspace ONE delivers tailored integrations for key industries, enabling specialized device management and workflows critical to frontline and regulated environments. This provides customers with a platform that meets unique operational, compliance and workflow needs across industries.

- **Product strategy:** Omnissa is the only vendor in the Leaders quadrant for both endpoint management tools and DEX management tools. The combination of these tools results in a unified platform that enhances device performance, employee experience and endpoint management efficiency.

Cautions

- **Organizational stability:** Omnissa (formerly VMware EUC) was acquired by Broadcom in November 2023 and subsequently acquired by KKR in July 2024. As a result of these changes, the organization experienced several disruptions that led to Gartner client reports of challenges with service and sales. Now independent and stabilized, Omnissa is actively rebuilding relationships and its reputation as a global endpoint management leader.

- **Sales execution/pricing:** Though it offers modular options for specific use cases, Workspace ONE pricing is on the higher end among vendors in this Magic Quadrant. Omnissa also does not alter its sales strategy for target customer roles or personas. Higher overall suite pricing can result in increased difficulties closing deals.

- **Customer experience:** Omnissa features very few customer case studies related to Workspace ONE on its website. A lack of published case studies and reference accounts can signal limited proof of success, making it harder to evaluate real-world impact or justify investment.

Raynet

Raynet is a Niche Player in this Magic Quadrant. Founded in 1999, it is a privately held company headquartered in Paderborn, Germany, with operations primarily located in Europe.

Its endpoint management tool, Raynet One for Unified Endpoint Management (UEM), supports Windows, macOS, iOS/iPadOS (through partnership with AppTec360), Android (Enterprise, OEMConfig and AOSP, through partnership with AppTec360), ChromeOS, and Linux. The platform offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises, customer cloud hosting (AWS and Azure) and turnkey SaaS. Vendor-provided geographical hosting options are available in the United States and Germany.

Raynet did not provide details on its licensing model.

Strengths

- **Geographic strategy:** Raynet has a strong geographical focus on the DACH region (Germany, Austria, Switzerland), where it has deep roots and a well-established customer base. The company originated in Germany and continues to prioritize the DACH market through localized support and services and a strong presence in the public sector, manufacturing and healthcare verticals that are common in the region.

- **ITAM focus:** Raynet One has a strong focus on IT asset management (ITAM) capabilities, helping organizations reduce risk, optimize costs and improve compliance by delivering a single source of truth for all IT assets. Raynet One Technology Catalog provides comprehensive visibility into hardware, software and vulnerability data.

- **Sales strategy:** Raynet utilizes a diversified sales channel strategy, with equal focus on direct sales, resellers and MSPs. It also uses a differentiated sales strategy aligned to buyer personas, increasing flexibility and relevance for prospective customers.

Cautions

- **Product:** Raynet One scored poorly in 12 of 15 Critical Capabilities, with notable limitations in macOS support, first-party mobile device management and automation and workflow orchestration. Documentation is limited, which can create challenges for customers trying to fully understand and implement platform capabilities.

- **Marketing execution:** Raynet's limited marketing is ITAM-focused and sometimes challenging for endpoint management buyers to fully understand the capabilities of

Raynet One. Gartner client interactions indicate that customer awareness of Raynet is low, which may impact growth.

- **Sales execution/pricing:** Raynet does not publicly disclose list prices or packaging information for Raynet One. A lack of transparency on deal structures and list pricing can hinder customer budgeting, comparison and procurement decisions, and challenge customers' ability to ensure they are receiving the best deal possible.

Samsung Electronics

Samsung Electronics is a Niche Player in this Magic Quadrant. Founded in 1969, it is a privately held company headquartered in Seoul, South Korea, with globally distributed operations.

Its endpoint management tool, Samsung Knox Suite, supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig and AOSP), ChromeOS (limited), and Linux. The platform does not offer a repository of prepackaged applications for simplified deployment. It is hosted via turnkey SaaS, with geographical hosting options in the United States and Ireland.

Samsung Knox Suite is licensed per device, with available tiers including Base Plan, Essentials Plan and Enterprise Plan.

Strengths

- **Overall viability:** Samsung Electronics is a large, diversified organization with globally distributed operations. Growing and profitable, its largest deployment is over 2.2 million devices, the most of all vendors in this Magic Quadrant.

- **Market understanding:** Samsung Knox Suite is focused on mobile device management, with deep capabilities in managing Samsung Knox mobile devices and hardware-embedded Samsung Knox security. These features help customers manage dedicated and shared device fleets securely and efficiently across multiple use cases.

- **Sales execution:** Samsung Electronics relies extensively on resellers, wireless carriers and MSPs to sell Samsung Knox Suite. This approach gives prospective customers flexibility to select the purchasing channel that best fits their procurement preferences, existing vendor relationships and operational needs.

Cautions

- **Marketing execution:** Samsung Electronics primarily positions the Samsung Knox Suite as a gateway to access and leverage the advanced capabilities of its Galaxy devices. While many clients are familiar with Samsung and its Knox security features for smartphones, Gartner client interactions indicate that awareness of Samsung Knox Suite specifically is low, which may impact growth.

- **Product:** Samsung Knox Suite's core value lies in its Galaxy hardware, which has zero-trust-ready security and manageability as a stand-alone product or a complementary solution with other endpoint management tools. Although it supports basic use cases for Windows and macOS, its capabilities for these platforms may not fully meet enterprise needs. Prospective customers should thoroughly evaluate Samsung Knox Suite's features to ensure compatibility with their requirements.

- **Geographic strategy:** Samsung Electronics offers limited hosting options for Knox Suite, with options only in the United States and Ireland. This limits data residency options and may create compliance challenges for organizations with strict regional hosting or data sovereignty requirements.

Tanium

Tanium is a Leader in this Magic Quadrant. Founded in 2007, it is a privately held company headquartered in Emeryville, California, U.S., with globally distributed operations.

Its endpoint management tool, Tanium Endpoint Management, supports Windows, macOS and Linux device management. It offers a repository of prepackaged applications for simplified deployment. Hosting options include on-premises and turnkey SaaS. Geographical hosting options include the United States, Canada, Germany, the United Kingdom, Brazil, Australia and Japan. Tanium Endpoint Management holds FedRAMP (Moderate) certification.

Tanium Endpoint Management is licensed per device, with available tiers including Endpoint Management Standard and Plus.

Strengths

- **Product:** Tanium provides real-time discovery, policy enforcement, software deployment and patching for Windows, macOS and Linux devices. Its advanced AEM capability reduces operational overhead, improves security posture through continuous compliance, and protects the employee experience during updates.

- **Operations:** Tanium is profitable and growing rapidly. It provides operational capabilities in all major geographies, has achieved all relevant security and privacy certifications, and offers flexible geographic hosting options. Tanium's roadmap is developed using structured and continuous feedback loops directly aligned to customer needs. As a result, Tanium delivers a compliant and globally scalable solution that meets complex enterprise requirements.

- **Marketing execution:** Tanium effectively delivers a high volume of thought-leading materials through multiple channels. Its AEM-focused content resonates with customers, resulting in high company and customer awareness among Gartner clients.

Cautions

- **Sales execution/pricing:** Tanium recently restructured its product bundling to include more capabilities in the endpoint management bundles. However, its list pricing is on the higher end of all vendors in this Magic Quadrant. Customers should carefully evaluate the value of included capabilities against their specific needs and budget.

- **Mobile device management:** While on its roadmap, Tanium does not currently offer mobile device management as a first-party capability. The company offers integration with Microsoft Intune. Customers with mobile device management requirements who are not using Intune should monitor Tanium's progress on this capability.

- **macOS management:** Tanium does not offer mobile device management or declarative device management support for Apple macOS. It provides legacy support for configuration management, operating system and application patching, and deployment via a custom process rather than Apple's modern methodologies. As a result, customers may face limitations in scalability, automation and compliance when managing macOS devices.

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.

As this is an inaugural Magic Quadrant, no vendors were added or dropped.

Added

Dropped

Inclusion and Exclusion Criteria

To qualify for inclusion in this Magic Quadrant, endpoint management vendors must provide the following as of 1 August 2025:

- Agent-based or agentless management for any of these operating systems:

  - Apple iOS and iPadOS

  - Apple macOS

  - Google Android

  - Microsoft Windows (client versions)

- Support for all the following core features on one or more of the above operating systems:

  - Application deployment (must be proprietary [first-party] intellectual property and must not require the use of any third-party or OEM products or external partnerships).

  - Device configuration and policy enforcement through a graphical user interface with predefined selectable options (must be proprietary [first-party] intellectual property and must not require the use of any third-party or OEM products or external partnerships).

  - Device enrollment and provisioning.

  - OS patching and update management.

- A product that operates as a turnkey SaaS (vendor hosted and operated; not IaaS; not entirely on-premises).

- A product with role-based access controls (RBACs) that provide granular administrative permissions, enabling dedicated support teams to manage their portion of the

environment.

- Evidence that the endpoint management product has at least 5 million active endpoints under management, excluding managed endpoints entitled under trial, freemium or other no-cost use arrangements.

- Rank in the top 20 qualified vendors in Gartner's Customer Interest Indicator (CII) compiled by Gartner's Secondary Research Service for this market in August 2025.

Honorable Mentions

The criteria for inclusion of platform providers in this Magic Quadrant are based on a combination of quantitative and qualitative measures, as noted in the Inclusion and Exclusion Criteria section. Below are several noteworthy providers that did not meet all the inclusion criteria but could be appropriate for clients, contingent on requirements. The following is a nonexhaustive list, presented in alphabetical order:

Aagon: Aagon supports full life cycle management of Windows, macOS and Linux devices through its modular ACMP platform. It features automated vulnerability management, customizable workflows, asset and license management, and strong alignment with DACH-region compliance and data protection standards for secure, localized control. Aagon did not meet the inclusion criteria for 5 million active endpoints under management.

Addigy: Addigy supports macOS, iOS and iPadOS with cloud-native tools for streamlined device management and compliance. It also features real-time zero-trust security enforcement through its proprietary Apple-first Security Suite with integrated EDR and MDR. Addigy did not meet the inclusion criterion for 5 million active endpoints under management.

Applivery: Applivery supports management of iOS, iPadOS, macOS, Android and Windows devices. It features an AEM capability that utilizes AI to automate provisioning, patching and policy enforcement, as well as comprehensive eSIM management for mobile devices. Applivery did not meet the inclusion criterion for 5 million active endpoints under management.

Automox: Automox supports endpoint management for Windows, macOS and Linux. Its platform enables rapid, automated software updates and real-time policy enforcement across endpoints without requiring VPNs or on-premises infrastructure. Automox did not meet the inclusion criterion for 5 million active endpoints under management or the criterion for device enrollment and provisioning.

Fleet: Fleet provides management for Windows, macOS, Linux, Android and iOS devices through a scalable, open-source platform. It features GitOps automation, real-time visibility and community-driven extensibility for cost-efficient and highly customizable control. Fleet did not meet the inclusion criterion for 5 million active endpoints under management.

Hexnode: Hexnode supports management for Windows, macOS, Linux, Android, iOS and ChromeOS. It features zero-touch deployment, unified policy control and remote troubleshooting with real-time device access. Hexnode did not meet the inclusion criterion for 5 million active endpoints under management.

Iru: Iru, formerly Kandji, provides management for Apple devices and has recently added management for Windows and Android devices. It features zero-touch deployment, automated application updates for over 200 applications, and over 150 prebuilt security automations that automatically restore settings that drift out of compliance. Iru did not meet the inclusion criterion for 5 million active endpoints under management.

Matrix42: Matrix42 supports management of Windows, macOS, Linux, Android and iOS devices. It features AI-driven automation, remote support, and strong alignment with DACH-region compliance and data sovereignty standards for secure, localized control. Matrix42 did not meet the inclusion criterion for 5 million active endpoints under management.

Scalefusion: Scalefusion supports management of Windows, macOS, Linux, Android, iOS and ChromeOS devices. Alongside traditional device management features, it provides frontline workers with support for kiosk modes, remote troubleshooting, and dynamic policy enforcement for rugged, shared devices. Scalefusion did not meet the inclusion criterion for 5 million active endpoints under management.

Splashtop: Splashtop supports management of Windows, macOS, Linux, Android, iOS and ChromeOS devices. It features AI-powered vulnerability insights, autonomous endpoint management, real-time patch automation that includes third-party applications, a change management automation framework, and self-healing endpoint capabilities for efficient IT operations. Splashtop did not meet the inclusion criterion for device enrollment and provisioning.

Evaluation Criteria

Ability to Execute

Gartner evaluates factors such as the vendor's product development, overall viability, market responsiveness, sales channels, customer experiences and customer base to determine a vendor's ability to execute.

General evaluation criteria are available at the bottom of this research. For this market, assessments were primarily based on:

Product or service: Evaluates core products offered by the vendor that compete in or serve the defined market. This includes current product capabilities, quality, feature sets and documentation in multiple product categories including Windows, macOS, iOS, Android, Linux, and ChromeOS management and patching, as well as ancillary support, reporting, hosting, and specialty device management.

Overall viability: The overall viability assessment evaluates an organization's financial health and the success of its business unit, focusing on its ability and willingness to continue investing in endpoint management. Factors include organizational size, profitability, liquidity, and the business unit's market position, revenue contribution, customer retention, growth in endpoint management sales, and acquisition of new customers.

Sales execution/pricing: Evaluates a provider's presales capabilities and supporting structure, including deal management, pricing, negotiation, presales support, and sales channel effectiveness. Key factors include customer support during sales, use of direct and indirect channels, and pricing. Pricing carries the most weight, assessing model flexibility and actual price performance.

Market responsiveness/record: Measures a vendor's agility and responsiveness to evolving market dynamics, customer needs, regulations, and competitor actions. It assesses flexibility, ability to change direction, and history of adapting to market demands. Vendors were evaluated on the maturity of their endpoint management capabilities and their actions over the past 12 months to address emerging requirements.

Marketing execution: Assesses the clarity, creativity, and impact of marketing programs that build brand awareness and influence market perception. Evaluation includes recent campaigns, thought leadership, social media, publicity, and promotional activities. Factors considered: ability to stand out, measure impact, leverage press and events, and demonstrate substance over quantity. Brand depth, global equity and effectiveness in attracting buyers were also key considerations.

Customer experience: Evaluates products, services, and programs that help customers achieve expected outcomes, including technical and account support, tools, user groups, and SLAs. Factors include quality of customer relationships, support programs, and processes for incorporating feedback. Direct customer input from Gartner Peer Insights and other sources was also considered.

Operations: Assesses the ability of the organization to meet goals and commitments. Factors include the overall size and quality of the organizational structure, skills, experiences, programs, systems, and other vehicles that enable the organization to operate effectively and efficiently. We also evaluated organizational changes, certifications and internal processes, as well as availability (in terms of uptime) for SaaS-based offerings.

Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	High

Source: Gartner (January 2026)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to understand current market opportunities and create and articulate their vision for future market direction, innovation, customer requirements, and competitive forces. Ultimately, vendors are rated on their vision for the future, and how well that maps to Gartner's position.

General evaluation criteria are available at the bottom of this research. For this market, assessments were primarily based on:

Market understanding: Evaluates products, services, and programs that help customers achieve expected outcomes, including technical and account support, tools, user groups, and SLAs. Factors include quality of customer relationships, support programs, and processes for incorporating feedback. Direct customer input from Gartner Peer Insights and other sources was also considered.

Marketing strategy: Assesses whether vendor messaging is clear, differentiating, and consistently communicated internally and externally through media, advertising, and customer programs. Evaluation includes communication plans for promoting endpoint management initiatives and products, marketing organization competitiveness, and planned media use to convey messaging effectively.

Sales strategy: Assesses the soundness of a vendor's sales strategy, including use of direct and indirect channels and partner networks to expand reach, expertise, and customer base. Evaluation covers multichannel sales approaches and the vendor's ability to enable and support its internal and external sales force.

Offering (product) strategy: Assesses a vendor's product development and delivery strategy, focusing on differentiation, functionality, and alignment with current and future requirements. Heavy weight was given to the top three roadmap features. Evaluation also considered plans to meet customer selection criteria, catch up with competitors, and deliver unique value through product strategy.

Business model: Assesses the strength of a vendor's business strategy, including clarity of its growth plan, understanding of competitive strengths and weaknesses, and recent milestones. Evaluation also covers ability to build and leverage partnerships with adjacent technologies, resellers, and integrators, as well as ease of doing business from a customer perspective.

Vertical/industry strategy: Assesses a vendor's strategy to allocate resources and offerings to meet specific market segment needs, including midsize enterprises, service providers,

and verticals. Evaluation includes applicability to industries, understanding of segment requirements, and planned vertical strategy changes. Innovation is also assessed, focusing on technical and nontechnical advancements that improve privileged access management and differentiate products, as well as strategic resource deployment for investment or competitive positioning.

Geographic strategy: Assesses a vendor's strategy and ability to expand beyond its home geography through direct operations, partners, channels and subsidiaries. Evaluation includes international market presence, plans to grow global sales and support, product internationalization, and availability of localized services and support across regions.

Completeness of Vision Evaluation Criteria

Evaluation Criteria	*Weighting*
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Medium
Innovation	High
Geographic Strategy	High

Source: Gartner (January 2026)

Quadrant Descriptions

Leaders

Leaders exhibit strong execution and vision scores and exemplify the functionality required for IT organizations to manage their endpoint device fleets. They have the broadest set of capabilities, the strongest roadmaps, a larger installed base, and coverage of the most geographic regions and industries.

Challengers

Challengers exhibit a strong set of technologies, marketing and sales execution, and intellectual property, as also exhibited by Leaders, but do not have the requisite strategic support, vision, innovation, or roadmap to compete in the Leaders quadrant. Many tailor solutions to specific market segments or use cases.

Visionaries

Visionaries exhibit strong strategic support, vision, innovation, and a robust roadmap, but have not yet amassed the requisite size, installed base, platform breadth, or integration points to compete in the Leaders quadrant.

Niche Players

Niche Players consistently address specific use cases, geographic regions, market segments, or verticals. However, their offerings fail to provide a breadth of features and cannot scale to be relevant to all buyers.

Context

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 review the accompanying Critical Capabilities research to review use case and functionality requirements, and this research to align industry expertise, vision, technology, and cost requirements to the right vendor, regardless of the vendor's quadrant.

Market Overview

The endpoint management market is very mature, with a few vendors holding significant market share. However, Gartner clients often use competitive or complementary tools alongside their primary (usually UEM) tool to address gaps or augment missing/underperforming capabilities.

Gartner expects moderate, top-line market growth for the next few years until mainstream modern-management-based UEM tools address functionality gaps when compared with traditional management client-based tools. These gaps tend to be around speed, reliability and granularity, which significantly increase the overhead of performing endpoint operations.

Several differentiating factors should be considered when evaluating vendors and tools in this market. They include the breadth and depth of capabilities to address the following:

Intelligence-Driven, Autonomous Capabilities Are Driving This Market

The rapid evolution of SaaS-powered capabilities, integration of threat intelligence data, the elevated importance of DEX tools and use cases, and the rapid advancement of AI/ML and generative AI are paving the path toward the next generation of endpoint management tools.

Gartner predicts that, within the next three years, demand for autonomous actions will be driven by IT leaders' and MSPs' inability to scale staffing levels and skill sets to meet demand. This has resulted in many vendors implementing AEM within their products. Although currently focused on intelligence-driven patch automation, Gartner expects AEM to include configuration and policy management, among other workloads, within the next few years.

OS Management

- Microsoft Windows represents over 90% of the client PC OS market (see **Forecast: PCs, Tablets and Mobile Phones, Worldwide, 2023-2029, 4Q25**). As a result, most vendors prioritize support for Windows and have the strongest capabilities to manage it.

- Enterprise interest in and adoption of Apple macOS remains steady. New adopters frequently manage macOS with existing UEM tools; however, organizations that have had

a large number of Macs for a long time commonly manage them with specialized Apple management tools.

- Despite once being a strong, stand-alone market, enterprise mobile management (EMM) or MDM for devices running Apple iOS, iPadOS and Android has become commoditized, with little differentiation between offerings.

- While some UEM tools lack mobile application management (MAM) support, many still secure corporate data through containerized apps or integration with Microsoft Entra and Intune policies. These protections apply with or without MDM enrollment, and MAM is most commonly used for BYOD.

Configuration Management

- Endpoint configuration helps digital workplace leaders stay compliant with organizational, security and regulatory standards, and is a core feature of endpoint management tools.

- Polling, data capture, and reporting capabilities vary significantly between tools, often resulting in gaps and accuracy issues with UEM tools that primarily rely on modern management capabilities. Agent-based tools tend to offer more frequent and accurate reporting, which is needed for compliance analysis and configuration/remediation efforts.

- IT leaders in regulated industries can benefit from endpoint management tools that offer prebuilt configuration templates and compliance reporting against common cybersecurity frameworks.

Application Management

- IT leaders are looking for ways to deploy, update, patch and remove applications, as well as manage the full application life cycle.

- IT leaders are also looking to reduce IT administration overhead by leveraging a catalog of prepackaged third-party applications, and rapidly redeploying updates and patches via integration with endpoint management tools.

- An AEM approach to application patching is desired to greatly reduce the labor and time traditionally required for this activity.

Hosting Options

- Most organizations seek a cloud-first approach, which puts SaaS-hosted endpoint management tools in high demand. These tools are best positioned to support almost all organizations.

- In response to demand for data sovereignty, many vendors have established robust hosting offerings.

- Although not as popular as SaaS, on-premises, private cloud, and highly secured SaaS-hosted offerings are still needed for high-security, highly regulated, or cloud-averse organizations, or for air-gapped network use cases. These include varying degrees of integration and usually do not have feature parity with their SaaS counterparts.

Organizational Fit

- **Willingness to embrace automation:** When considering the advanced capabilities of AEM and increased automation within endpoint management tools, it is important to consider whether the organizational culture is in alignment. Organizations with rigid change control processes and very low tolerance for potential impact generally receive less value from tools with advanced automation capabilities, due to a fundamental conflict between the need for control and the desire to increase velocity.

- **Number of endpoints:** Organizations with a large number of endpoints to manage must carefully evaluate the vendor's capability to scale to meet their needs.

- **Required integrations and partnerships:** Integration capabilities with adjacent tools and platforms, including identity, access and endpoint security management tools, as well as IT service management (ITSM) platforms, should be evaluated to ensure seamless operation.

- **Regulatory and security certifications:** To prevent significant cybersecurity risk exposure and potential regulatory fines, organizations in high-security or regulated industries must ensure that the vendor's compliance and security certifications meet their requirements.

- **Endpoint management team maturity and skill set:** The skill set and level of organizational maturity within the endpoint management team should also be taken into account to avoid overbuying tools from which the team will be challenged to extract value. Many organizations incorrectly assume that the most complete tool is the best fit for them, but tools alone are insufficient. For maximum success and value, ensure that the

endpoint management team has both the capability and desire to use the sophisticated features of advanced endpoint management tools.

Looking Ahead

Gartner sees the following forces shaping the future of the endpoint management tool market:

- A greater focus on AEM to increase automation and maintain DEX as a result of operations. AEM significantly reduces visibility gaps that hinder operations by providing near-real-time application, device and employee sentiment analysis.

- Common acceptance of hybrid and remote work, which is increasing demand for improved, location-agnostic patching and endpoint management. This emphasizes the increased importance of SaaS-hosted tools.

- Integration with vulnerability assessment, endpoint analytics and endpoint security tools to build proactive and resilient defenses for endpoints.

Acronym Key and Glossary Terms

⊕ Evidence

Notes

⊕ Evaluation Criteria Definitions

statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner's Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Gartner.

Get The App

GET IT ON Google Play   Download on the App Store