Critical Capabilities for Endpoint Management Tools

5 January 2026 - ID G00826086 - 50 min read

By: Lina Al Dana, Tom Cipolla, Sunil Kumar, Robin Milton-Schonemann, Craig Fisler, Todd Larivee

Initiatives:Digital Workplace Infrastructure and IT Operations

Endpoint management tools are essential to manage, secure and enable employee computing devices. I&O leaders should use this research to guide endpoint management tool investment.

This Critical Capabilities is related to other research:

Magic Quadrant for Endpoint Management Tools

View All Magic Quadrants and Critical Capabilities

Overview

Key Findings

- Endpoint management tools are evolving rapidly with the integration of AI/ML, threat intelligence and digital employee experience (DEX) capabilities. These advancements enable autonomous actions that help organizations overcome staffing limitations and improve operational resilience.
- Gartner clients continue to report that traditional change, patch and update processes are too slow to meet operational demands. As organizations accelerate delivery, maintaining DEX and operational resilience remains a persistent challenge.
- Unified endpoint management (UEM) offerings in the market are mature and feature-rich, providing broad support for managing diverse device fleets. However, limitations in patching speed, reporting capabilities and support for nonstandard devices often require organizations to augment UEM with OS-specific or niche tools for platforms such as macOS, ChromeOS, Android, specialty devices, kiosks and Linux.
- Vendors are increasingly integrating endpoint management tools with vulnerability management and endpoint security platforms. These integrations support risk-based remediation by enabling prioritized patching based on vulnerability severity and asset criticality, helping organizations reduce risk exposure and improve patching efficiency.

Recommendations

- Evaluate endpoint management vendors based on their ability to support scalable, autonomous operations that reduce reliance on manual processes and align with evolving workforce and infrastructure demands.
- Reduce the time associated with endpoint management and protect DEX by leveraging intelligence-driven automation within a ring-based approach, accelerated by real-time operational DEX (OpDEX) metrics provided by autonomous endpoint management (AEM) powered tools.
- Reduce complexity and total cost of ownership (TCO) by standardizing on a UEM platform for core capabilities, while using OS-specific tools to ensure fast patching and reliable configuration management where UEM falls short.
- Shortlist endpoint management tools that integrate with existing vulnerability and endpoint security platforms in your environment to enable closed-loop patch detection, remediation and validation, thereby improving efficiency and reducing risk exposure.

What You Need to Know

Endpoint management tools primarily support four key use cases, which form the foundation of this research. These include unified endpoint management, autonomous endpoint management, security-centric management, and frontline device management. Each use case is defined below in the Use Cases section and includes both must-have and nice-to-have critical capabilities.

Each tool is evaluated against a consistent set of capabilities and scored across the same use cases. IT leaders should carefully assess each vendor that aligns with their high-level requirements such as OS support, application management, patching, reporting, hosting and automation (workflow orchestration) capabilities. Integration with adjacent platforms, such as ITSM, vulnerability management, endpoint security and DEX tools, is essential to ensure operational efficiency and alignment with enterprise IT strategies.

Critical Capabilities research differs from Magic Quadrant research, which focuses on overall vendor positioning in the endpoint management tool market. Instead, the Critical Capabilities report emphasizes how each tool aligns with and supports the most critical capabilities and use cases.

Gartner recommends using the interactive version of this research to adjust capabilities and weightings to reflect your unique needs. Our analysis synthesizes vendor-provided product information, generally available functionality as of 1 August 2025 and Gartner client feedback from the past year.

Analysis

Critical Capabilities Use-Case Graphics

Figure 1: Vendor Product Scores for the Unified Endpoint Management Use Case

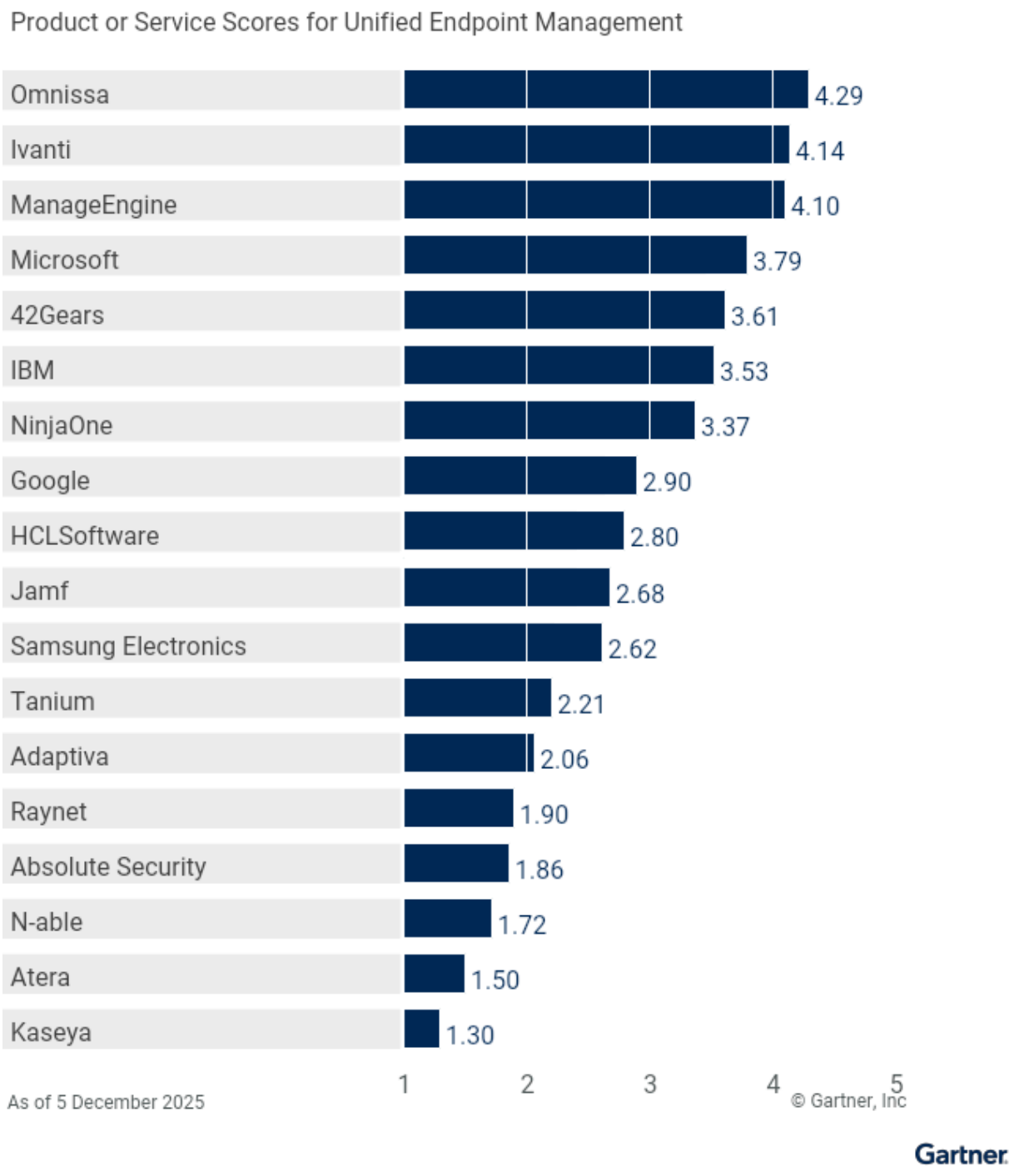


Figure 2: Vendor Product Scores for the Autonomous Endpoint Management Use Case

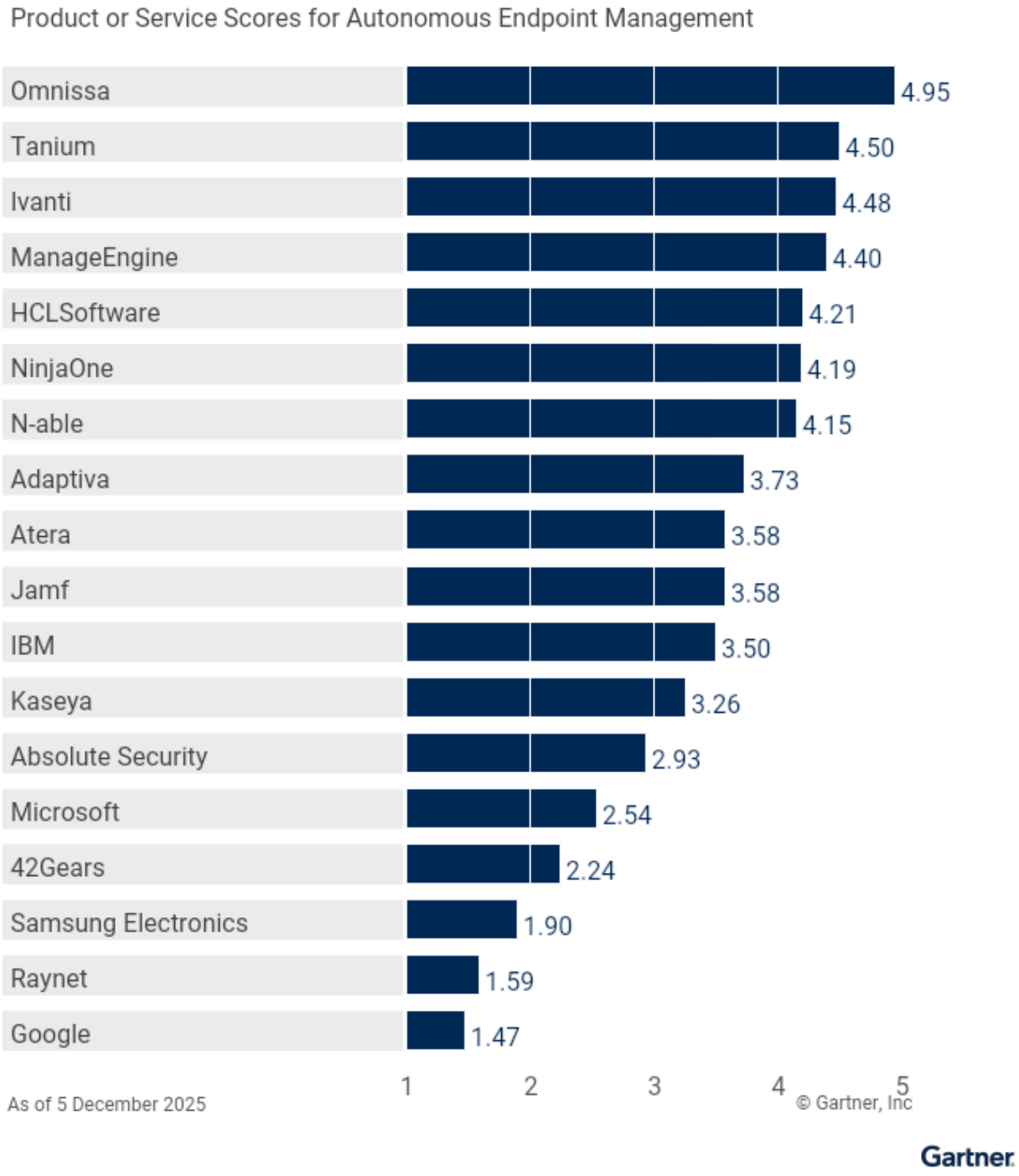


Figure 3: Vendor Product Scores for the Security-Centric Management Use Case

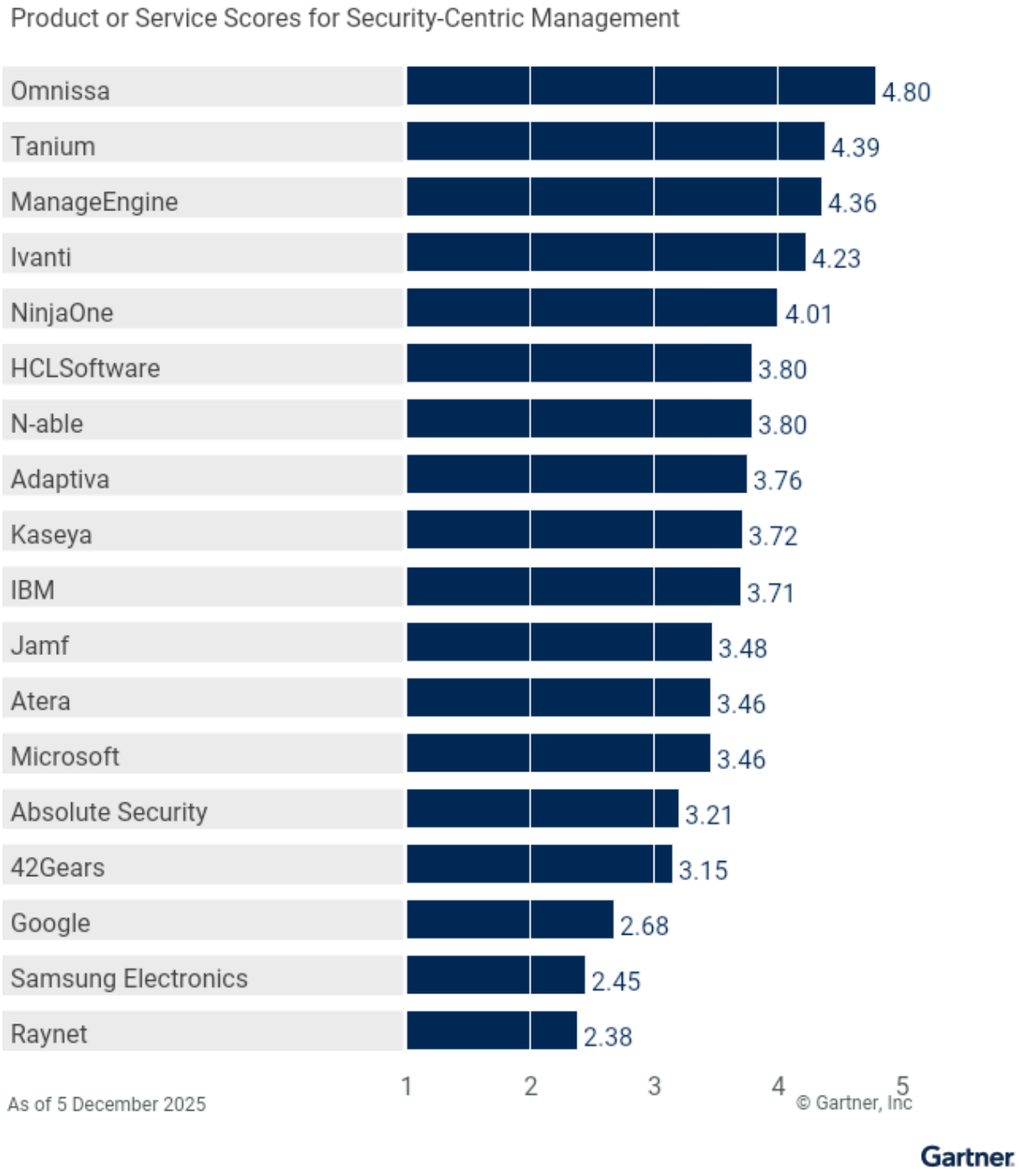
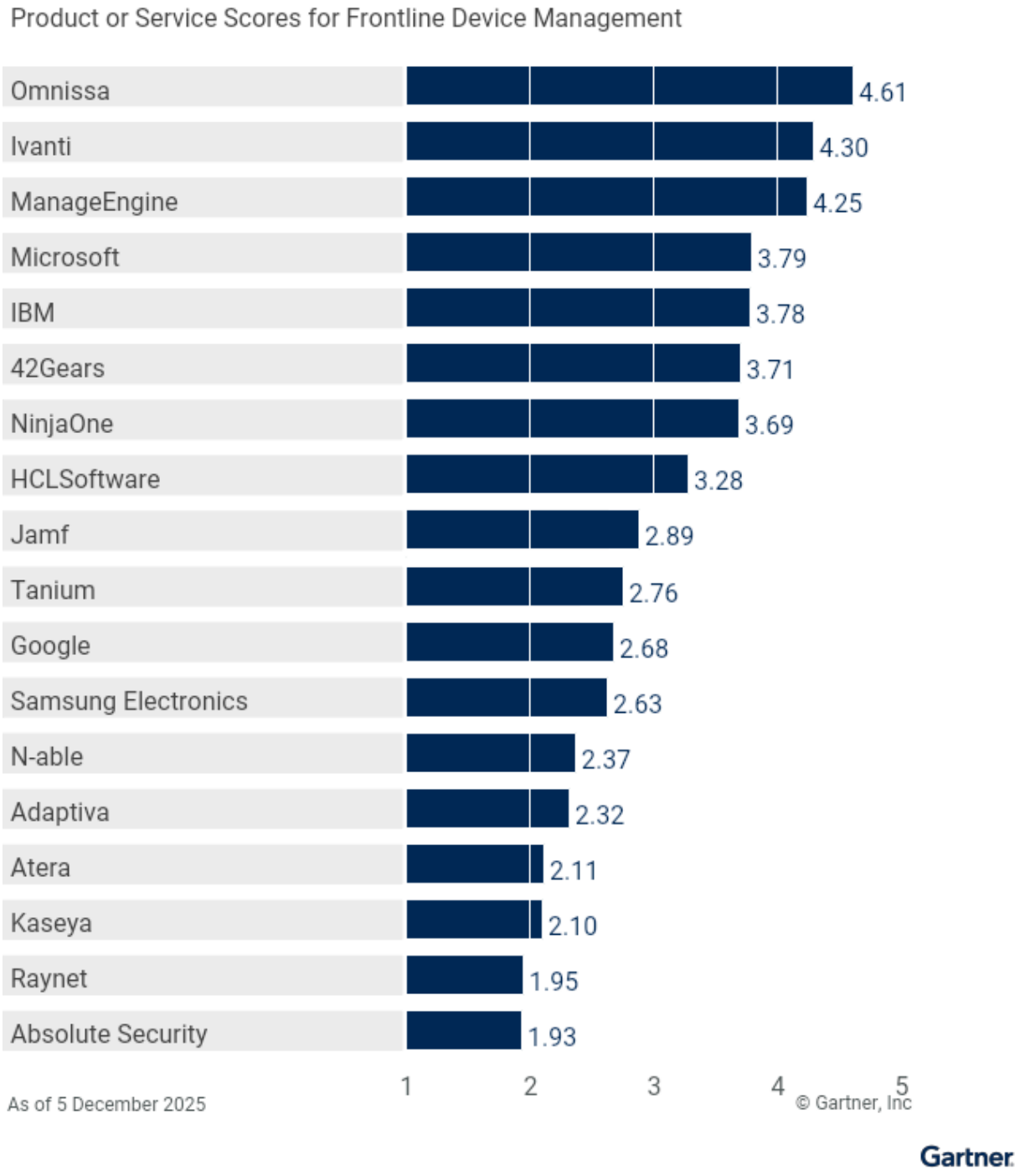


Figure 4: Vendor Product Scores for the Frontline Device Management Use Case



Vendors

42Gears

SureMDM is offered as SaaS (multitenant and dedicated instance), vendor-hosted and on-premises. Customers can determine the geographic region where their data is hosted. It supports Windows, macOS, iOS/iPadOS, Google Android (Enterprise, OEMConfig and AOSP), Linux and ChromeOS platforms. It also offers a mobile application management (MAM)-only approach, allowing organizations to manage and secure apps without requiring full device enrollment.The solution includes capabilities for specialty devices, rugged devices, shared devices and kiosks, with support for Zebra LifeGuard OTA, Samsung Knox and other OEM-specific tools. 42Gears primarily targets verticals such as financial services, retail, healthcare and manufacturing. It also primarily targets small and midsize businesses (SMBs) and midmarket organizations, but has scaled to serve organizations of all sizes, from small businesses to extra-large enterprises, across North America, Europe and the Asia/Pacific region. 42Gears has achieved regional and industry certifications including GDPR, CCPA/CPRA, HIPAA, PCI DSS and SOC 2 Type II.

The platform includes a centralized console for managing multiple endpoint types, remote support capabilities and indoor location tracking, and provides built-in mobile threat defense (MTD). It incorporates generative AI to assist with script creation to streamline the creation of management scripts, allowing administrators to automate complex tasks using natural language input, which can reduce manual effort and improve consistency in policy enforcement.

It integrates with ServiceNow ITSM and endpoint security tools such as Microsoft Defender. SIEM systems like Splunk and ArcSight are supported as well.**Critical Capabilities Summary**

42Gears rated a 3 (meets requirement) or higher in all but one of its critical capabilities.

The highest-rated capabilities were shared device/kiosk management and specialty device management, boosted by full AOSP and OEMConfig support, rugged device compatibility, and single app and multiapp kiosk support for Windows, Linux, iOS and Android.

The lowest-rated capabilities was automation (workflow orchestration), due to the absence of centralized orchestration and a low-code/no-code workflow designer.

Use Case Summary

The highest-scored use case was frontline device management, driven by strong ratings in shared device/kiosk management and specialty device management capabilities.

Its lowest-scored use case was autonomous endpoint management, due to limited automation capabilities restricted to basic, manual bulk task execution without centralized orchestration.

Absolute Security

Absolute Secure Endpoint Resilience for Automation is offered as SaaS (multitenant and dedicated instance). Customers can determine the geographic region where their data is hosted. The solution supports Windows, macOS and Linux OS, with limited support for ChromeOS. It doesn't support automated device provisioning via Windows Autopilot and Apple Business Manager. Absolute Security primarily targets regulated verticals such as financial services, healthcare, government, education and small to large enterprises across North America, Europe and South America.

Absolute Security has achieved certifications including FedRAMP (moderate), ISO 27001 and SOC 2 Type II.

The platform supports unified IT and SecOps automation and is built on a secure multitenant architecture. The solution provides security- and compliance-oriented reports, including patch risk assessment, patch deployment and detected vulnerabilities reports. HIPAA, SOC and PCI reports are also available for patch compliance. The platform integrates with Absolute Security's vulnerability management capabilities as part of the Absolute Resilience framework. This integration enables coordinated workflows, such as vulnerability detection, automated patch deployment and endpoint self-healing, within a unified console.

It integrates with ITSM platforms from ServiceNow and ConnectWise, and DEX tools such as ServiceNow DEX, Lakeside SysTrack and Omnissa Workspace ONE Intelligence. It also integrates with vulnerability management tools like Microsoft Defender, Qualys, Rapid7 and Tenable for patching and compliance.

Critical Capabilities Summary

Its highest-rated capability was hosting capabilities, which include support for geographic data residency across all supported Azure regions. This includes hosting in the U.S. with FedRAMP certification for federal customers, enabling compliance with stringent government security standards.

The lowest-rated capabilities were iOS/iPadOS management, Android management, specialty device management and shared device/kiosk management, as these are currently not supported by the platform. The solution provides partial support for ChromeOS through integration with the Google Admin console. It enables monitoring, reporting and remote freeze/location functions, but policy enforcement actions must be configured directly within the Google Admin console.

Use Case Summary

Its highest-scored use case was security-centric management, driven by deep integration with leading security tools and robust hosting capabilities enabling compliance with federal standards and data residency requirements across global jurisdictions.

Its lowest-scored use cases were unified endpoint management and frontline device management, primarily due to the platform's lack of support for mobile devices, specialty, and shared device and kiosk configurations.

Adaptiva

Adaptiva OneSite is offered as SaaS (multitenant and dedicated instance), vendor-hosted, and on-premises. Customers can determine the geographic region where their data is hosted. It supports Windows, macOS and Linux endpoints. It doesn't support automated device provisioning via Windows Autopilot or Apple Business Manager. The vendor targets organizations of all sizes across all verticals, with a focus on financial services, manufacturing and professional services and large to extra-large enterprise organizations in North America, Europe and the Asia/Pacific region.

Adaptiva OneSite has achieved regional certifications including GDPR, EU-U.S. Data Privacy Framework, Swiss-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. Data Privacy Framework.

The platform provides peer-to-peer content delivery and autonomous endpoint management capabilities including sensor-based endpoint analytics for visibility into device health and compliance, and low/no-code workflow automation designer. AI/ML capabilities include generative and agentic AI, which enable asset discovery, natural language reporting and automated patch strategy execution, reducing manual effort and accelerating risk-based remediation.

It integrates with ServiceNow ITSM and endpoint security tools such as Microsoft Defender, CrowdStrike Falcon, Tenable One and SentinelOne. Integration with Microsoft Intune is also supported.

Critical Capabilities Summary

Adaptiva's highest-rated capabilities were multitenancy support and RBAC, and Linux OS management and patching. Multitenancy is offered for managed service providers (MSPs), with clear separation of admins and devices. Its Linux management supports major distributions such as Ubuntu, Debian, RHEL and CentOS. Capabilities include centralized monitoring, application deployment and compliance enforcement.

The lowest-rated capabilities were iOS/iPadOS management, Android management, ChromeOS management and patching, specialty device management, and shared device/kiosk management, which are currently not supported by the platform.

Use Case Summary

The highest-scored use case was security-centric management, driven by the platform's extensibility and integration with security and vulnerability management tools and its robust reporting capabilities.

The lowest-scored use case was unified endpoint management, due to the lack of support for mobile device management, ChromeOS, specialty devices, and shared device and kiosk environments.

Atera

Atera is offered as SaaS (multitenant) and customers can determine the geographic region where their data is hosted. It supports Windows, macOS and Linux platforms, and includes capabilities for shared devices and SNMP-enabled specialty devices. It doesn't support automated device provisioning via Windows Autopilot or Apple Business Manager. The vendor primarily targets MSPs and IT departments across verticals including healthcare, retail, manufacturing, education, and government, and small to medium enterprise organizations in North America and Europe.

Atera has achieved regional and industry certifications, including SOC 2 Type II, GDPR, CCPA/CPRA compliance, HIPAA compliance and the ISO 27000 family.

The platform includes AI-based capabilities for diagnostics, remediation and natural language querying. It supports agentic and generative AI, along with automation for endpoint management tasks and an AI assistant for end users and technicians.The platform integrates with ITSM platforms from ServiceNow and Zendesk, and endpoint security tools such as Bitdefender and ESET. Integration with Vicarius vulnerability management is also supported.**Critical Capabilities Summary**

Its highest-rated capability was multitenancy support and RBAC, enabled through the use of sites and roles to manage device access and administrative functions. While not true multitenancy, MSPs can organize customers with granular permissions.

Its lowest-rated capabilities were iOS/iPadOS management, Android management, ChromeOS management and patching, and shared device/kiosk management, as these are currently not supported by the platform.

Use Case Summary

Its highest-scored use case was security-centric management supported by strong reporting capabilities, which include detailed auditor reports and customizable analytics dashboards for deeper data insight. High ratings in endpoint analytics, automation (workflow orchestration), and extensibility and integration contributed to the platform's overall effectiveness in supporting security-centric management.Its lowest-scored use case was unified endpoint management, due to the solution's lack of support for mobile devices, ChromeOS, and shared device and kiosk configurations.

Google

Google Endpoint Management is offered as SaaS hosted on Google Cloud Platform (GCP) infrastructure. It serves as the native solution for managing ChromeOS devices. It supports Android, iOS/iPadOS and Windows, and includes capabilities for rugged devices, shared devices and kiosks, with limited support for macOS and Linux OS devices. The vendor primarily targets the education vertical and organizations of all sizes globally.

Google has achieved regional and industry certifications, including FedRAMP High P-ATO, GDPR, HIPAA, the ISO 27000 family and PCI DSS.

It provides native capabilities within Google Workspace and supports Apple Business Manager and Apple School Manager. Single-app and multiapp kiosk management for iOS and Android is supported. It offers basic MAM features for iOS, including selective wipe and app-level controls. Similar capabilities are supported for Android devices through the use of Android Work Profiles, enabling separation of personal and work data.

It supports integration with ITSM platforms such as ServiceNow and Jira through Google SecOps and API connectors. Patch workflows can be orchestrated via Google SecOps playbooks and third-party EDR integrations. Endpoint security and vulnerability management are supported via integrations with CrowdStrike and SentinelOne.

Critical Capabilities Summary

Its highest-rated capability was ChromeOS management and patching, as it supports all core ChromeOS management functions natively, including device enrollment, policy enforcement and patching.

Its lowest-rated capabilities were endpoint analytics and remote support and control, driven by the lack of built-in performance analytics and dashboards for endpoint health scoring. Remote support is limited to basic actions such as remote signout and wipe, with no interactive control of devices.

Use Case Summary

Its highest-scored use case was unified endpoint management, boosted by its high rating for ChromeOS management and patching and its broad support for other OSs and device types, including mobile devices, specialty devices, and shared device and kiosk configurations.

Its lowest-scored use case was autonomous endpoint management, due to its limited endpoint analytics and automation (workflow orchestration) capabilities.

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

HCLSoftware

HCL BigFix Workspace+ is offered as a vendor-hosted, on-premises and SaaS offering. Customers can determine the geographic region where their data is hosted. It supports Windows, macOS, Linux OS, iOS/iPadOS and Android (Enterprise), and includes capabilities for shared devices and kiosks. The vendor primarily targets financial services, government, technology and telecom, retail, and healthcare verticals, and large to extra-large enterprise organizations in North America, Europe and the Asia/Pacific region.

HCLSoftware has achieved regional and industry certifications, including the ISO 27000 family, GDPR, CCPA/CPRA, SOC 2 Type II and PCI DSS.

The platform incorporates advanced capabilities including autonomous endpoint management, which enables continuous policy enforcement and self-healing operations across managed devices. It also captures endpoint performance metrics and provides contextual insights by correlating telemetry with external data sources such as CMDB, and supports automation through AI-driven recommendations and low-code orchestration.

It integrates with a wide range of external systems, including ServiceNow for ITSM and ITAM; endpoint security platforms such as Symantec, McAfee and Trend Micro; and vulnerability management tools like Tenable, Qualys and Rapid7. It also connects with SIEM solutions including Splunk and IBM QRadar.

Critical Capabilities Summary

Its highest-rated capabilities were endpoint analytics and Linux OS management and patching, boosted by telemetry and application diagnostics across distributed environments. The platform supports configuration and patching for major Linux distributions, including RHEL, CentOS, Oracle Linux, SLES and Ubuntu.Its lowest-rated capabilities were ChromeOS management and patching and specialty device management, as both are not supported by the platform.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, boosted by HCL BigFix Workspace+ capabilities such as HCL BigFix AEX and HCL BigFix Runbook AI, which enable low-code orchestration across reactive, proactive and predictive workflows. Automation triggers include policy violations, scheduled compliance checks and AI-driven anomaly detection, while human-initiated actions are supported via an admin console and the AEX agentic-AI-led conversational platform. This is complemented by granular endpoint analytics, including device experience metrics.

Its lowest-scored use case was unified endpoint management, due to its lack of support for ChromeOS and specialty devices.

IBM

IBM MaaS360 is offered as SaaS (multitenant and dedicated instance) and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig, AOSP), ChromeOS, specialty devices and kiosk configurations. iOS Declarative Device Management (DDM) is also supported.

The vendor primarily targets financial services, manufacturing, retail, healthcare, government verticals, and small businesses to medium enterprises across North America, Europe and the Asia/Pacific region.

IBM has achieved regional and industry certifications, including FedRAMP (Moderate), GDPR, the ISO 27000 family, SOC 2 Type II, CCPA/CPRA and NIST SP-800-171.

Key platform capabilities include AI/ML-driven insights, GenAI for policy recommendations and agentic AI for prompt-based smart portal advisors. It also provides automation via Action Orchestrator, compliance rule enforcement and real-time telemetry-based remediation. MAM is supported for iOS and Android. Data loss prevention (DLP) policies can be enforced across managed devices.

The solution integrates with a wide range of systems, including ServiceNow for ITSM, Flexera and Maximo for ITAM, and Tenable for vulnerability management. It also supports integration with endpoint security platforms such as CrowdStrike, SentinelOne and ReaQta. Additional integrations include peer-to-peer transfer tools such as Aspera and DEX platforms like Lakeside Software and TeamViewer.

Critical Capabilities Summary

IBM rated a 3 (meets requirements) or higher in all but three of its critical capabilities.

Its highest-rated capability was hosting capabilities, which include support for geographic data residency across several regions, including hosting in the U.S. with FedRAMP (Moderate) certification for federal customers, enabling compliance with stringent government security standards. Additionally, the platform has achieved a broad set of regional and industry certifications.

Its lowest-rated capability was Linux OS management and patching, primarily due to limited native support for Linux within the platform.

Use Case Summary

Its highest-scored use case was frontline device management, boosted by the capabilities for specialty devices such as wearables, Apple TV and custom devices like printers, as well as shared devices and kiosks, with features like a Kiosk Designer for configuring kiosk experiences via a drag-and-drop interface.

Its lowest-scored use case was unified endpoint management, driven by lower ratings for ChromeOS management and patching and Linux OS management and patching.

Ivanti

Ivanti Neurons for Unified Endpoint Management (UEM) is offered as SaaS (multitenant and dedicated instance), vendor-hosted, and on-premises (with the legacy Ivanti Endpoint Manager) and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig, AOSP), ChromeOS and limited Linux OS management capabilities. It also includes capabilities for shared devices, kiosks and rugged/frontline worker devices. DDM for iOS and macOS devices is supported.

The vendor primarily targets manufacturing, retail, healthcare, financial services and government verticals, and midmarket to extra-large enterprise organizations in North America, Europe and the Asia/Pacific region.

Ivanti has achieved regional and industry certifications, including FedRAMP Moderate, GDPR, ISO 27701, CCPA/CPRA, EU-U.S. Data Privacy Framework, SOC 2 Type II and PCI DSS. The solution provides autonomous remediation workflows that automatically detect, diagnose and resolve endpoint issues. Autonomous endpoint management capabilities extend to automated patch impact analysis using patch intelligence combined with sentiment analysis and policy-based enforcement. It supports MAM for Android and iOS, enabling secure app deployment, configuration and access control on both corporate and BYOD devices.The solution supports extensibility and integration with Ivanti's other products, such as Ivanti Neurons for ITSM and Ivanti Neurons for ITAM; external systems such as ServiceNow ITSM; and vulnerability management tools from CrowdStrike, Qualys, Rapid7 and Microsoft.

Critical Capabilities Summary

Ivanti rated a 3 (meets requirement) or higher in all but one of its critical capabilities.

Its highest-rated capabilities were endpoint analytics, iOS/iPadOS management and Android management, driven by a telemetry engine that collects and presents granular device-level data. The platform uses over 80 quantitative sensors with hundreds of data points. Its mobile management capabilities include DDM for iOS, MAM, split tunneling VPN and built-in MTD.

Its lowest-rated capability was Linux OS management and patching, which currently lacks support for application deployment, kiosk mode configuration, and remote shell scripting or SSH access.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, boosted by high ratings for endpoint analytics and automation (workflow orchestration), which includes a low/no-code designer and a wide variety of out-of-the-box templates for automation.

Its lowest-scored use case was unified endpoint management, but it still scored a 4 (meets or exceeds some requirements).

Jamf

Jamf is offered as SaaS, vendor-hosted and on-premises, and customers can determine the geographic region where their data is hosted. It primarily supports macOS, iOS/iPadOS, Android (Enterprise and OEMConfig), with limited ChromeOS support, and includes capabilities for shared devices and kiosks. The vendor primarily targets the education, healthcare, financial services, transportation and utilities verticals, and organizations of all sizes in North America, Europe and the Asia/Pacific region.

Jamf has achieved regional and industry certifications, including the ISO 27000 family, GDPR, SOC 2 Type II and CCPA/CPRA.

The solution provides deep integration with the Apple ecosystem, like Apple Business Manager, Automated Device Enrollment, and Platform SSO and custom configuration and scripts. For mobile devices, it includes capabilities such as MAM, split tunneling VPN, geofencing and network change monitoring.

Specialty device management includes Apple TV, Apple Watch, and Apple Vision Pro and Zebra devices.It supports integration with ITSM platforms such as Freshservice ITSM, HaloITSM and SolarWinds Service Desk. Integration with endpoint security tools such as Microsoft Defender and CrowdStrike Falcon are supported as well. Jamf also provides MTD capabilities with its mobile offering.

Critical Capabilities Summary

Its highest-rated capabilities include macOS management and patching and reporting capabilities, driven by its depth of functionality for macOS devices. It also offers security-focused reporting features such as threat view, device view, vulnerability insights and customizable reports, including data usage and security events.

Its lowest-rated capabilities were Windows management and patching, Linux OS management and patching, and ChromeOS management and patching. Windows and Linux OS are not supported, while ChromeOS support is limited to content filtering, web protection configurations and usage reporting.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, boosted by higher ratings for endpoint analytics and automation (workflow orchestration) capabilities, which include autonomous actions powered by intelligence-driven data and a low/no-code designer.

Its lowest-scored use case was unified endpoint management, primarily due to the lack of support for Windows and Linux OS and lack of configuration capabilities for ChromeOS.

Kaseya

Datto RMM is offered as SaaS (multitenant and dedicated instance), vendor-hosted and on-premises, and customers can determine the geographic region where their data is hosted. It supports Windows, macOS and Linux OS. It doesn't support automated device provisioning via Windows Autopilot and Apple Business Manager.

The vendor primarily targets MSPs, midmarket organizations and the public sector in North America, Europe and the Asia/Pacific region.

Kaseya has achieved regional and industry certifications, including SOC 2 Type II and GDPR.

The solution is built primarily for MSPs and as an RMM that supports multitenancy, RBAC and monitoring capabilities. It also supports workflow orchestration through automation policies and integrations with human-initiated, reactive, proactive and predictive triggers. The automations within Datto RMM can be configured within a centralized workflow designer.

The solution supports extensibility and integration with Kaseya's other products such as KaseyaOne and Kaseya 365, external systems including ITSM and ITAM from Autotask and ServiceNow, and endpoint security tools from Bitdefender and Sophos.

Critical Capabilities Summary

Kaseya rated below a 3 (meets requirements) for more than half of the critical capabilities.

Its highest-rated capability was reporting capabilities, boosted by dynamic dashboarding with prebuilt filters for segmentation and analysis across device health and compliance and performance metrics. Reports can be created and scheduled to be delivered on a repetitive basis.

Its lowest-rated capabilities were iOS/iPadOS management, Android management, ChromeOS management and patching, specialty device management, and shared device/kiosk management, as these are currently not supported by the solution.

Use Case Summary

Its highest-scored use case was security-centric management, due to its higher ratings in endpoint analytics, automation (workflow orchestration) and reporting capabilities.

Its lowest-scored use case was unified endpoint management, driven by its lack of support for mobile device management, ChromeOS, specialty devices, and shared devices and kiosks. Datto RMM supports Windows, macOS and Linux, and relies on the usage of prebuilt scripts and automation packages (components) available through its ComStore, with the option to create custom components as needed.

ManageEngine

ManageEngine Endpoint Central is offered as SaaS (multitenant and dedicated), vendor-hosted and on-premises, and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, Linux, iOS/iPadOS, Android (Enterprise, OEMConfig, AOSP) and ChromeOS, and includes capabilities for shared devices, kiosks and rugged/specialty devices. DDM is supported for macOS and iOS.

The vendor targets a wide variety of industry verticals, including regulated industries such as healthcare, financial services and government, and small businesses to medium enterprise organizations in all regions.

ManageEngine has achieved regional and industry certifications, including the ISO 27000 family, SOC 2 Type II, GDPR, CCPA/CPRA and the U.K.'s Cyber Essentials Plus.

The platform offers a unified agent and centralized console that streamlines endpoint management, security enforcement and experience telemetry across supported OSs. It enables advanced automation through a low-code workflow builder, and delivers equally comprehensive configuration and patch management capabilities for Windows, macOS, Linux, iOS/iPadOS, Android and ChromeOS environments, including MAM capabilities for mobile devices.

It supports integration with ITSM platforms from ServiceNow, Jira, Zendesk and Freshservice, and vulnerability management tools from Tenable, Rapid7 and CrowdStrike. Integration with SIEM systems such as Splunk and Log360 are also supported.

Critical Capabilities Summary

ManageEngine rated a 3 (meets requirements) or higher for all critical capabilities.

Its highest-rated capabilities were multitenancy support and RBAC and specialty device management, including rugged devices, kiosks and shared endpoints. RBAC can limit access based on roles, functional responsibilities, device groups and physical locations.

Its lowest-rated capabilities were remote support and control and extensibility and integration, but they still were rated a 3 (meets requirements) or higher.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, driven by strong ratings in endpoint analytics and automation (workflow orchestration). Its visual workflow builder enables proactive, reactive and predictive automation, supporting self-healing actions, root cause analysis and orchestration.

Its lowest-scored use case was unified endpoint management; however, it scored higher than a 4 (meets or exceeds some requirements), indicating that core requirements were met or surpassed.

Microsoft

Microsoft Intune is offered as SaaS and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig, AOSP) and Linux, and includes capabilities for shared devices, kiosks and frontline worker devices. DDM is supported for macOS and iOS devices. Microsoft targets organizations in all verticals, sizes and geographic regions.

Microsoft has achieved regional and industry certifications, including FedRAMP (High), the ISO 27000 family, GDPR, SOC 2 Type II, IL5, ISO 27701, NIST SP-800-171, PCI DSS, and various data privacy frameworks (e.g., EU-U.S., Swiss-U.S., UK Extension to the EU-U.S. Data Privacy Framework).

The platform provides a unified management console to manage all OSs, including mobile device capabilities that include MAM, MAM without enrollment (MAM-WE), and app protection policies to protect corporate data and employee privacy across managed and unmanaged devices. The solution supports extensibility and integration with ITSM platforms from ServiceNow, BMC, Ivanti and Atlassian. It also integrates with Microsoft Defender for Endpoint and third-party MTD tools from CrowdStrike, Zimperium and Pradeo. Remote control/support, advanced endpoint analytics, and enterprise application management and other features are available within the Microsoft Intune Suite add-on.

Critical Capabilities Summary

Its highest-rated capabilities were iOS/iPad OS management and Android management. This was boosted by support for MAM and MAM-WE, including app protection policies that safeguard corporate data at the application level within managed Microsoft 365 apps and other third-party applications for corporate and BYOD. DLP can be enforced on mobile devices, and split tunneling VPN is supported.

Its lowest-rated capability was ChromeOS management and patching, which is limited to basic inventory visibility and remote actions (wipe, restart, lost mode) after syncing with Google Workspace.

Use Case Summary

Its highest-scored use case was unified endpoint management, driven by its capabilities to fully manage all major OSs. The only exceptions were ChromeOS and Linux, which offer limited actions and configuration management capabilities.

Its lowest-scored use case was autonomous endpoint management, primarily due to limited capabilities in automation (workflow orchestration) and endpoint analytics.

N-able

N-able N-central is offered as SaaS (multitenant and dedicated), vendor-hosted and on-premises, and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, Linux and iOS/iPadOS. The vendor primarily targets small to midmarket organizations and MSPs across North America and Europe.

N-able has achieved regional and industry certifications, including SOC 2 Type II, GDPR, CCPA/CPRA and PCI DSS.

The platform provides integrated analytics and reporting, including access to Report Manager with more than 60 SQL-based reports. Dashboards for patch compliance are also available, and automation is supported through a low/no-code workflow builder with more than 700 prebuilt scripts, AI-assisted scripting and dynamic, telemetry-based triggers. The platform also supports advanced remote troubleshooting, including remote control, chat, back-end service diagnostics, application uninstallation, command-line access, file transfers, script execution, registry access and multimonitor support across Windows, macOS and Linux.

It supports integration with ITSM platforms from ServiceNow, Halo and TOPdesk, and endpoint security tools such as those from SentinelOne and Bitdefender. Integration with DEX tools from Nexthink, Lakeside and TeamViewer are also supported.

Critical Capabilities Summary

Its highest-rated capabilities were multitenancy support and RBAC and hosting capabilities, due to geographical hosting available in almost every country worldwide and multitenancy available for all customers.

Its lowest-rated capabilities were Android management, ChromeOS management and patching, specialty device management, and shared device/kiosk management, as these are currently not supported.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, due to its high ratings in endpoint analytics and automation (workflow orchestration). The platform offers over 100 prebuilt monitoring service templates and more than 700 customizable workflow elements. It supports PowerShell, VBScript and Bash, but most tasks require no scripting. Automation can be triggered manually, reactively, proactively or predictively

Its lowest-scored use cases was unified endpoint management, driven by its lack of support for Android, ChromeOS, specialty devices, and shared devices and kiosks. While N-able N-central supports macOS management, it uses configuration profiles created by third-party tools for configuration management and DDM is also not supported.

NinjaOne

NinjaOne Endpoint Management is offered as SaaS (multitenant and dedicated instance) and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, Linux, iOS/iPadOS and Android (Enterprise and OEMConfig) platforms. The solution includes capabilities for shared devices, kiosks and rugged/specialty devices. DDM is supported for macOS.

The vendor primarily targets the professional services, media, personal and consumer services, utilities, and transportation verticals, including government. It also targets small to midmarket organizations, with growing adoption in small and midsize enterprises.

NinjaOne has achieved regional and industry certifications, including FedRAMP (Moderate Authorized), GDPR SOC 2 Type II, ISO 27001:2022 and CCPA/CPRA.

The platform provides patching through an AI-built safety score (Patch Intelligence AI), which uses public data from the internet and evaluation of patching results. The platform collects both quantitative telemetry and qualitative user sentiment survey data to generate a DEX score. This data is analyzed to deliver actionable insights and recommendations for improving user experience and operational performance. MAM for mobile devices is also supported.

The solution supports extensibility and integration with ITSM platforms from ServiceNow and Zendesk, and endpoint security tools such as CrowdStrike Falcon and SentinelOne. Integration with vulnerability management tools from Qualys, Rapid7 and Tenable to drive prioritized patching is also supported.

Critical Capabilities Summary

NinjaOne rated a 3 (meets requirements) or higher for all but three capabilities.

Its highest-rated capability was automation (workflow orchestration), driven by a low-code/no-code orchestration engine through its automations, enabling visual workflow design with drag-and-drop functionality and dynamic script forms, which allow technicians to customize scripts without editing code.

Its lowest-rated capability was ChromeOS management and patching, which is limited to inventory tracking and warranty status. Configuration and patch management are not supported.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, due to its integration of low/no-code automation, AI-assisted patching and self-healing workflows.

Its lowest-scored use case was unified endpoint management; however, it scored higher than a 3 (meets requirements), indicating that core requirements were met.

Omnissa

Omnissa Workspace ONE UEM is offered as SaaS (multitenant and dedicated instance) and on-premises (by exception only), and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, iOS/iPadOS, Android (Enterprise, OEMConfig, AOSP), Linux and ChromeOS, and includes capabilities for rugged devices, shared devices and kiosks. DDM for macOS and iOS is supported. The vendor primarily targets the federal government, financial services, healthcare, public sector, retail and education verticals, and organizations of all sizes globally.

Omnissa has achieved regional and industry certifications, including FedRAMP, the ISO 27000 family, SOC 2 Type II, SOC 3, GDPR, CCPA/CPRA and the U.K.'s Cyber Essentials Plus.

The platform provides automated patching and vulnerability remediation through integrations like CrowdStrike, enabling faster response to security exposures. Telemetry from endpoints is collected via Workspace ONE Experience Analytics to assess performance and user experience. Workspace ONE also includes low-code orchestration through Freestyle Orchestrator for automating IT workflows, and supports multitenant configurations for complex environments. Its mobile management capabilities include DDM for iOS, MAM, split tunneling VPN and built-in MTD.

The solution supports extensibility and integration with ITSM platforms from ServiceNow and TOPdesk, and endpoint security tools from CrowdStrike, Microsoft, Pradeo and Lookout. Integration with SIEM tools from Splunk and Tenable are also supported.

Critical Capabilities Summary Omnissa rated a 3 (meets requirements) or higher for all its capabilities.

Its highest-rated capabilities were endpoint analytics, automation (workflow orchestration), and multitenancy and RBAC, boosted by a wide range of collection telemetry and insight, its low/no-code orchestration engine Freestyle Orchestrator, and its capabilities to support multitenancy for complex organizations and MSPs.

Its lowest-rated capability was ChromeOS management and patching;however, it scored higher than a 3 (meets requirements), indicating that core requirements were met.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, due to its higher ratings for endpoint analytics and automation (workflow orchestration), which rated a 5 (outstanding: significantly exceeds requirements).

Its lowest-scored use case was unified endpoint management, due to its lower score for ChromeOS management and patching. However, this use case scored higher than a 4 (meets or exceeds some requirements), indicating that core requirements were met or surpassed.

Raynet

Raynet One for Unified Endpoint Management (UEM) is offered as SaaS (multitenant and dedicated instance), vendor-hosted and on-premises, and customers can determine the geographic region where their data is hosted. It supports Windows, Linux, macOS, and ChromeOS. iOS/iPadOS and Android (Enterprise, OEMConfig and AOSP) management are supported through a partnership with AppTec360. It doesn't support automated device provisioning via Windows Autopilot and Apple Business Manager. The vendor targets all verticals and large to extra-large enterprises in primarily Europe and North America.

Raynet has achieved regional and industry certifications, including GDPR and the ISO 27000 family.

The platform provides inventory data, including software overviews, vulnerability insights and end-of-life software reporting. Users can build custom reports through an interactive interface, with support from the RaynetAI assistant to query data and generate dashboards. These capabilities enable streamlined visibility and reporting across managed endpoints. Raynet One offers unified endpoint management capabilities, but it does not include native mobile device management functionality. These capabilities are instead delivered through integration with AppTec360.

The solution supports extensibility and integration with ITSM platforms such as ServiceNow ITSM and HaloITSM, and endpoint security tools from CrowdStrike. Raynet One integrates with CrowdStrike via the Raynet One Data Connector. The integration enables asset data from Raynet One to be supplemented with vulnerability information and security posture indicators. It also supports continuous asset discovery and shares data with CrowdStrike to improve visibility into endpoint configurations and tool deployment status.

Critical Capabilities Summary

Raynet rated below 3 for all but three of its capabilities.

Its highest-rated capability was hosting capabilities, which include support for geographic data residency in Europe, the U.S. and Asia regions.

Its lowest-rated capabilities were macOS management and patching, as MDM, DDM and Apple Business Manager are not supported. Traditional client management tool management is supported.

Use Case Summary

Its highest-scored use case was security-centric management, due to its reporting capabilities and integration with endpoint security tools such as CrowdStrike.

Its lowest-scored use case was autonomous endpoint management, driven by lower ratings for endpoint analytics and automation (workflow orchestration).

Samsung Electronics

Samsung Knox Suite is offered as SaaS (multitenant and dedicated instance), vendor-hosted and on-premises, and customers can determine the geographic region where their data is hosted. It supports Windows, macOS, iOS/iPadOS, Android (Enterprise and OEMConfig) and ChromeOS platforms, and includes capabilities for specialty devices (Samsung devices) and kiosks.

The vendor primarily targets the public sector (including government agencies), education, retail and transportation verticals, and large and extra-large enterprise organizations, in Europe, North America and the Asia/Pacific region.

Samsung Electronics has achieved regional and industry certifications, including GDPR, ISO 27001:2013, CCPA/CPRA and SOC 2 Type II.

The solution provides cloud-based analytics for Samsung devices via Knox Asset Intelligence, requiring a Knox account and a supported Knox version. The dashboard displays battery health, device status and background app usage. Data views are customizable, with alert thresholds and access to historical trends. It also provides ChromeOS management by interfacing with Google Admin console via Google APIs. Policy changes, OS updates and device enrollment are supported and reflected in Knox Manage. Android OEMConfig support capabilities are available for Samsung devices only. Wear OS management for Samsung watches is also supported.

The solution supports extensibility and integration with external systems such as Microsoft Intune, Microsoft Sentinel, Omnissa Workspace ONE, SOTI MobiControl, ServiceNow ITSM and SAP. Zimperium, Check Point Software Technologies and Pradeo are supported for MTD.

Critical Capabilities Summary

Its highest-rated capability was multitenancy support and RBAC, due to the granular role-based permission model. The separate Knox MSP portal enables creation of subadmins and fine-grained control over both internal and customer-facing permissions, supporting complex delegation and multitenant environments.

Its lowest-rated capabilities were Linux OS management and patching and automation (workflow orchestration), as Linux OS devices are not supported.

Use Case Summary

Its highest-scored use case was frontline device management, boosted by its kiosk management support capabilities, which include single and multi-app kiosk support for Windows and Android. Only single app kiosk support is available for iOS devices.Its lowest-scored use case was autonomous endpoint management, due to its low ratings in automation (workflow orchestration) and endpoint analytics capabilities, primarily driven by the absence of a low/no-code workflow designer. Endpoint analytics are restricted to Samsung devices with supported Knox versions.

Tanium

Tanium Endpoint Management is offered as on-premises and SaaS (dedicated instance), and customers can determine the geographic region where their data is hosted. It supports Windows and macOS. iOS/iPadOS and Android management is supported through integration with Microsoft Intune.

The vendor primarily targets the financial services, manufacturing, healthcare and government verticals, and large and extra-large enterprise organizations in North America, Europe and the Asia/Pacific region.

Tanium has achieved regional and industry certifications, including FedRAMP, the ISO 27000 family, GDPR, CCPA/CPRA, SOC 2 Type II and PCI DSS.

Tanium Endpoint Management provides autonomous endpoint management by combining real-time data collection, analysis and remediation across endpoints. It provides external and internal confidence scores to drive autonomous patching decisions by evaluating patch reliability based on real-world telemetry. External scores reflect success rates across Tanium's customer base, while internal scores assess performance within the organization's own environment, helping reduce patch failures and improve deployment safety.

The solution supports extensibility and integration with external systems such as ServiceNow ITSM, Microsoft Intune, Microsoft Defender for Endpoint and Microsoft Sentinel. It also integrates with other Tanium modules, such as Tanium Benchmark and Tanium Comply.

Critical Capabilities Summary

Its highest-rated capabilities were Windows management and patching and endpoint analytics, driven by deep capabilities for policy enforcement, OS and third-party patching for Windows devices. The Tanium Client collects a broad range of telemetry, including both quantitative metrics and qualitative data through sentiment surveys, and delivers actionable insights into the DEX, such as device performance, software usage patterns and user interaction trends.

Its lowest-rated capabilities were ChromeOS management and patching and shared device/kiosk management, as these are not currently supported.

Use Case Summary

Its highest-scored use case was autonomous endpoint management, driven by high ratings for endpoint analytics and automation (workflow orchestration) capabilities, which include capabilities to automate tasks across patching, compliance, software deployment and vulnerability remediation. Tasks are executed in a validated, step-by-step sequence using real-time telemetry from endpoints.

Its lowest-scored use case was frontline device management, due to the lack of support for specialty devices, shared devices and kiosks.

Context

The endpoint management market has remained relatively stagnant over the past several years, with most tools offering incremental improvements to long-established capabilities such as provisioning, patching and configuration. However, the rapid advancement of AI/ML is now catalyzing a significant transformation in this space. Vendors are accelerating innovation to meet modern demands for scalability, automation and risk reduction.

IT leaders evaluating endpoint management solutions are often seeking to consolidate legacy tools, reduce operational overhead and improve automation. The emergence of AEM — which leverages AI, DEX metrics and intelligence-driven automation — is reshaping expectations for endpoint operations, offering a path to reduce manual effort and improve responsiveness.

AEM has emerged as a key differentiator, introducing intelligence-driven automation that reduces manual effort, improves patch velocity and enhances DEX. AEM capabilities — including AI-powered patching decisions, telemetry-based configuration enforcement and sentiment-aware remediation — are reshaping how organizations manage endpoints. These tools help close visibility gaps, reduce operational overhead, and proactively mitigate security and compliance risks.

IT leaders must evaluate tools not only for traditional functionality, but also for their ability to support autonomous operations, integrate with security and identity platforms, and adapt to evolving workforce needs. Understanding the critical capabilities of endpoint management tools is essential for IT leaders to make informed investment decisions, align technology with organizational maturity and prepare for future demands in endpoint security, compliance and employee experience.

Market Definition

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

Product/Service Trends

The endpoint management tool market is undergoing a fundamental transformation, driven by the accelerated advancement of AI/ML and GenAI, growing emphasis on DEX, convergence of automation, evolving hybrid work requirements, and heightened security integration. Gartner analysis indicates that vendors are responding to these shifts by recalibrating their product strategies to address new enterprise priorities.

AEM is emerging as a core differentiator in the market. By leveraging AI, DEX metrics and intelligent automation, AEM significantly reduces operational labor and accelerates patching velocity. Gartner expects AEM capabilities to expand beyond patch automation to encompass configuration and policy management, enabling organizations to adjust automation levels according to risk appetite and compliance mandates. This evolution positions AEM as a key enabler of operational efficiency and improved security posture.

As hybrid and remote work models become normalized, the need for location-agnostic endpoint management has intensified. This trend is accelerating the adoption of SaaS-hosted endpoint management platforms, which provide turnkey management capabilities without reliance on VPN or corporate network access. Gartner research shows that SaaS delivery has become the preferred deployment model for most organizations, due to its scalability, ease of use and alignment with the demands of distributed workforces.

Integration with adjacent technologies is now a standard expectation among enterprise buyers. Endpoint management solutions increasingly incorporate or integrate with vulnerability assessment platforms, endpoint analytics and endpoint security solutions. These integrations enable proactive remediation, enrich telemetry and support zero-trust security postures, providing organizations with holistic visibility and improved risk mitigation.

Vendors are also introducing enhanced analytics and reporting capabilities to surface actionable insights. Real-time visibility into device health, application performance and employee sentiment is becoming essential for maintaining DEX and informing automation decisions. Gartner anticipates continued innovation in analytics and reporting as a driver of customer value and competitive differentiation.

These developments reflect a broader industry shift toward intelligent, resilient and user-centric endpoint operations. Vendors that do not incorporate autonomous management, SaaS delivery and robust security integrations risk losing relevance in a market that increasingly prioritizes agility, automation and digital experience. Gartner recommends that technology leaders evaluate endpoint management solutions based on their ability to support these imperatives and future-proof endpoint operations.

Critical Capabilities Definition

Windows Management and Patching

Ability to manage Windows devices with and/or without an agent. This includes device discovery, configuration, policy management, application deployment, device enrollment and provisioning, as well as OS and third-party application updates and patching.

macOS Management and Patching

Ability to manage macOS devices with and/or without an agent. This includes device discovery, configuration, policy management, application deployment, device enrollment and provisioning, as well as OS and third-party application updates and patching.

iOS/iPadOS Management

Ability to manage iOS/iPadOS mobile devices. This Includes application inventory, configuration management, encryption, root/jailbreak detection, automated device enrollment, OS updates, integration with app stores, remote wipe, software deployment and geolocation.

Also included is the ability to manage and secure corporate applications and data on iOS/iPadOS devices with or without device enrollment through MAM, featuring app-level data protection, selective wipe and policy-based access controls, without requiring full device management.

Android Management

Ability to manage mainstream Android mobile devices (excludes specialty devices). This includes application inventory, configuration management, encryption, root/jailbreak detection, automated device enrollment, OS updates, integration with app stores, remote wipe, software deployment and geolocation.

Also included is the ability to manage and secure corporate applications and data on Android devices with or without device enrollment through MAM, featuring app-level data protection, selective wipe and policy-based access controls, without requiring full device management.

Extensibility and Integration

Supports integration with external systems such as ITSM, security or ITAM systems to improve automation, compliance and visibility, or provides native ITSM, security and/or ITAM features within the tool.

Endpoint Analytics

Ability to collect and analyze telemetry from devices, applications, identity and connectivity to surface insights into endpoint performance and user experience. This Includes signal aggregation to identify trends, detect issues and inform data-driven decisions for experience optimization.

Automation (Workflow Orchestration)

Ability to provide a workflow orchestration engine and editor (preferably low/no code) to automate tasks and remediate issues across endpoints. This supports human-initiated, reactive, proactive and predictive triggers.

Also included is the ability to perform autonomous actions powered by intelligence-driven data and AI to augment IT operations and engineering.

Hosting Capabilities

Ability to host the endpoint management solution in customer-managed infrastructure or specific regions to meet data residency, sovereignty and regulatory requirements.

Linux OS Management and Patching

Ability to manage Linux devices with or without an agent. This includes device discovery, configuration, policy management, application deployment, device enrollment and provisioning, as well as OS and third-party application updates and patching.

ChromeOS Management and Patching

Ability to manage ChromeOS devices. This includes device discovery, configuration, policy management, application deployment, device enrollment and provisioning, as well as OS and third-party application updates and patching.

Multitenancy Support and RBAC

Ability to support multitenancy and provide RBAC. This enables secure, segmented management across organizational units or environments, with granular permission assignment based on roles and responsibilities. This supports delegated administration and operational scalability.

Specialty Device Management

Ability to configure, deploy, manage and support ruggedized devices across Android platforms. This includes support for OEM-specific management via Android OEMConfig and Android Open Source Project (AOSP).

Reporting Capabilities

Ability to generate standard, customizable and automated reports on endpoint hardware and software inventory, configuration and compliance status/anomalies, device status, ownership, and location.

Shared Device/Kiosk Management

Ability to configure and manage PC and mobile devices for limited-use scenarios such as kiosks, digital signage, utility, or shared use by students, frontline and task workers. Supports tailored access, session control and policy enforcement to ensure secure and consistent operation across shared environments.

Remote Support and Control

Ability to remotely view and control endpoints to support troubleshooting and issue resolution. Includes access to device inventory, performance metrics and stability data, enabling IT support staff to diagnose and resolve problems efficiently.

Use Cases

Unified Endpoint Management

The use of endpoint management tools to provide centralized, policy-based management of all endpoint devices.

This includes desktops, laptops, smartphones, tablets, IoT devices, wearables and rugged endpoints, across multiple OSs from a single console.

Autonomous Endpoint Management

The use of endpoint management tools to automate endpoint and DEX tasks using real-time data on configuration, compliance, risk, performance and experience.

AEM applies AI- and ML-driven automation to continuously assess endpoint state and autonomously execute actions such as patching, configuration updates, remediation and optimization — minimizing manual intervention and IT overhead.

Security-Centric Management

The use of endpoint management tools to enforce device policies focused on configuration, compliance and patching.

Automated patch deployment, encryption, threat detection and vulnerability management enable organizations to accelerate remediation of vulnerabilities and maintain continuous compliance. Seamless interaction with third-party security solutions — such as mobile threat defense (MTD), endpoint protection platforms (EPP), and endpoint detection and response (EDR) — ensures comprehensive protection across all endpoints.

Frontline Device Management

The use of endpoint management tools to centrally manage and secure frontline devices such as kiosks, shared workstations and specialty endpoints.

These devices are deployed in environments like retail, manufacturing, healthcare and logistics. Frontline device management enables IT teams to provision, configure and monitor devices that are often used by multiple users or operate in high-turnover, high-availability settings.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Critical Capabilities as markets change. As a result of these adjustments, the mix of vendors in any Critical Capability may change over time. A vendor's appearance in a Critical Capability 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 criteria, or of a change of focus by that vendor.

Added

No vendors have been added because this is a new Critical Capabilities report for this market.

Dropped

No vendors have been dropped because this is a new Critical Capabilities report for this market.

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.

Table 1: Weighting for Critical Capabilities in Use Cases

(Enlarged table in Appendix)

Critical Capabilities	*Unified Endpoint Management*	*Autonomous Endpoint Management*	*Security-Centric Management*	*Frontline Device Management*
Windows Management and Patching	15%	0%	0%	10%
macOS Management and Patching	15%	0%	0%	0%
iOS/iPadOS Management	15%	0%	0%	10%
Android Management	15%	0%	0%	10%
Extensibility and Integration	0%	10%	25%	5%
Endpoint Analytics	0%	45%	15%	10%
Automation (Workflow Orchestration)	0%	45%	15%	5%
Hosting Capabilities	0%	0%	10%	0%
Linux OS Management and Patching	10%	0%	0%	5%
ChromeOS Management and Patching	10%	0%	0%	0%
Multitenancy Support and RBAC	0%	0%	15%	5%
Specialty Device Management	10%	0%	0%	10%
Reporting Capabilities	0%	0%	20%	5%
Shared Device/Kiosk Management	10%	0%	0%	20%
Remote Support and Control	0%	0%	0%	5%
As of 5 December 2025				

Source: Gartner (January 2026)

This methodology requires analysts to identify the critical capabilities for a class of products/services. Each capability is then weighted in terms of its relative importance for specific product/service use cases.

Critical Capabilities Rating

Each of the products/services that meet our inclusion criteria has been evaluated on the critical capabilities on a scale from 1.0 to 5.0.

Table 2: Product/Service Rating on Critical Capabilities

(Enlarged table in Appendix)

Critical Capabilities	42Gears	Absolute Security	Adaptiva	Atera	Google	HCLSoftware	IBM	Ivanti	Jamf	Kaseya	ManageEngine	Microsoft	N-able	NinjaOne	Omnissa	Raynet	Samsung Electronics	Tanium
Windows Management and Patching	3.1	2.1	3.5	1.7	2.1	2.7	3.0	4.4	1.0	2.1	4.2	4.0	3.0	4.3	4.1	3.3	2.5	5.0
macOS Management and Patching	3.0	3.2	3.2	1.6	1.6	3.0	3.2	3.6	4.3	1.5	3.9	3.5	1.5	4.2	3.9	1.4	2.5	2.0
iOS/iPadOS Management	3.4	1.0	1.0	1.0	3.3	3.0	4.5	4.8	4.0	1.0	3.7	4.7	1.9	2.7	4.8	1.5	2.5	1.3
Android Management	3.3	1.0	1.0	1.0	3.4	3.1	4.5	4.8	3.3	1.0	3.8	4.8	1.0	2.7	4.8	1.5	3.3	1.3
Extensibility and Integration	3.5	2.3	3.1	2.9	2.1	2.9	3.0	3.8	2.9	3.8	3.5	4.2	2.8	4.1	4.5	2.4	1.9	4.5
Endpoint Analytics	3.2	2.8	3.7	3.5	1.0	4.8	2.9	4.8	3.3	3.9	4.5	2.8	3.9	3.9	5.0	1.5	2.7	5.0
Automation (Workflow Orchestration)	1.0	3.2	3.9	3.8	1.8	3.9	4.2	4.3	4.0	2.5	4.5	1.9	4.7	4.5	5.0	1.5	1.1	4.0
Hosting Capabilities	3.8	4.2	3.5	2.3	5.0	4.0	5.0	4.2	3.5	3.2	4.7	4.7	4.7	3.9	4.4	3.7	2.2	4.1
Linux OS Management and Patching	4.0	3.7	4.5	3.7	1.3	4.7	1.0	2.5	1.0	1.6	4.3	2.1	3.1	4.1	4.0	2.3	1.0	4.7
ChromeOS Management and Patching	3.4	1.9	1.0	1.0	4.9	1.0	2.7	3.9	1.2	1.0	4.1	1.8	1.0	1.3	3.6	2.1	3.4	1.0
Multitenancy Support and RBAC	4.0	4.1	4.5	4.3	4.2	3.5	5.0	3.8	3.1	4.2	4.8	3.4	4.8	4.1	5.0	2.0	3.9	3.5
Specialty Device Management	4.7	1.0	1.0	1.3	4.2	1.0	4.5	4.2	2.8	1.0	4.8	4.2	1.0	3.8	4.4	1.5	2.1	1.0
Reporting Capabilities	3.3	3.5	4.1	3.8	3.0	4.2	3.2	4.6	4.2	4.3	4.7	3.6	3.1	3.6	4.9	3.3	3.0	4.9
Shared Device/Kiosk Management	4.8	1.0	1.0	1.0	3.0	3.6	4.3	4.4	2.9	1.0	4.4	4.3	1.0	3.6	4.5	1.5	3.5	1.0
Remote Support and Control	3.8	2.0	1.8	2.7	1.1	2.8	3.2	3.4	2.1	3.5	3.5	2.3	3.3	4.1	4.5	2.8	1.4	2.4

As of 5 December 2025

Source: Gartner (January 2026)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use-case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3: Product Score in Use Cases

(Enlarged table in Appendix)

Use Cases	42Gears	Absolute Security	Adaptiva	Atera	Google	HCLSoftware	IBM	Ivanti	Jamf	Kaseya	ManageEngine	Microsoft	N-able	NinjaOne	Omnissa	Raynet	Samsung Electronics	Tanium
Unified Endpoint Management	3.61	1.86	2.06	1.50	2.90	2.80	3.53	4.14	2.68	1.30	4.10	3.79	1.72	3.37	4.29	1.90	2.62	2.21
Autonomous Endpoint Management	2.24	2.93	3.73	3.58	1.47	4.21	3.50	4.48	3.58	3.26	4.40	2.54	4.15	4.19	4.95	1.59	1.90	4.50
Security-Centric Management	3.15	3.21	3.76	3.46	2.68	3.80	3.71	4.23	3.48	3.72	4.36	3.46	3.80	4.01	4.80	2.38	2.45	4.39
Frontline Device Management	3.71	1.93	2.32	2.11	2.68	3.28	3.78	4.30	2.89	2.10	4.25	3.79	2.37	3.69	4.61	1.95	2.63	2.76
As of 5 December 2025																		

Source: Gartner (January 2026)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

Recommended by the Authors

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

How Products and Services Are Evaluated in Gartner Critical Capabilities

Table 1: Weighting for Critical Capabilities in Use Cases

Critical Capabilities	*Unified Endpoint Management*	*Autonomous Endpoint Management*	*Security-Centric Management*	*Frontline Device Management*
Windows Management and Patching	15%	0%	0%	10%
macOS Management and Patching	15%	0%	0%	0%
iOS/iPadOS Management	15%	0%	0%	10%
Android Management	15%	0%	0%	10%
Extensibility and Integration	0%	10%	25%	5%
Endpoint Analytics	0%	45%	15%	10%
Automation (Workflow Orchestration)	0%	45%	15%	5%
Hosting Capabilities	0%	0%	10%	0%
Linux OS Management and Patching	10%	0%	0%	5%
ChromeOS Management and Patching	10%	0%	0%	0%

Critical Capabilities	*Unified Endpoint Management*	*Autonomous Endpoint Management*	*Security-Centric Management*	*Frontline Device Management*
Multitenancy Support and RBAC	0%	0%	15%	5%
Specialty Device Management	10%	0%	0%	10%
Reporting Capabilities	0%	0%	20%	5%
Shared Device/Kiosk Management	10%	0%	0%	20%
Remote Support and Control	0%	0%	0%	5%
As of 5 December 2025				

Source: Gartner (January 2026)

Table 2: Product/Service Rating on Critical Capabilities

Critical Capabilities	*42Gears*	*Absolute Security*	*Adaptiva*	*Atera*	*Google*	*HCLSoftware*	*IBM*	*Ivanti*	*Jamf*	*Kaseya*	*ManageEngine*	*Microsoft*	*N-able*	*NinjaOne*	*Omnissa*	*Raynet*	*Samsung Electronics*	*Tanium*
Windows Management and Patching	3.1	2.1	3.5	1.7	2.1	2.7	3.0	4.4	1.0	2.1	4.2	4.0	3.0	4.3	4.1	3.3	2.5	5.0
macOS Management and Patching	3.0	3.2	3.2	1.6	1.6	3.0	3.2	3.6	4.3	1.5	3.9	3.5	1.5	4.2	3.9	1.4	2.5	2.0
iOS/iPadOS Management	3.4	1.0	1.0	1.0	3.3	3.0	4.5	4.8	4.0	1.0	3.7	4.7	1.9	2.7	4.8	1.5	2.5	1.3
Android Management	3.3	1.0	1.0	1.0	3.4	3.1	4.5	4.8	3.3	1.0	3.8	4.8	1.0	2.7	4.8	1.5	3.3	1.3
Extensibility and Integration	3.5	2.3	3.1	2.9	2.1	2.9	3.0	3.8	2.9	3.8	3.5	4.2	2.8	4.1	4.5	2.4	1.9	4.5

Endpoint Analytics	3.2	2.8	3.7	3.5	1.0	4.8	2.9	4.8	3.3	3.9	4.5	2.8	3.9	3.9	5.0	1.5	2.7	5.0
Automation (Workflow Orchestration)	1.0	3.2	3.9	3.8	1.8	3.9	4.2	4.3	4.0	2.5	4.5	1.9	4.7	4.5	5.0	1.5	1.1	4.0
Hosting Capabilities	3.8	4.2	3.5	2.3	5.0	4.0	5.0	4.2	3.5	3.2	4.7	4.7	4.7	3.9	4.4	3.7	2.2	4.1
Linux OS Management and Patching	4.0	3.7	4.5	3.7	1.3	4.7	1.0	2.5	1.0	1.6	4.3	2.1	3.1	4.1	4.0	2.3	1.0	4.7
ChromeOS Management and Patching	3.4	1.9	1.0	1.0	4.9	1.0	2.7	3.9	1.2	1.0	4.1	1.8	1.0	1.3	3.6	2.1	3.4	1.0
Multitenancy Support and RBAC	4.0	4.1	4.5	4.3	4.2	3.5	5.0	3.8	3.1	4.2	4.8	3.4	4.8	4.1	5.0	2.0	3.9	3.5
Specialty Device Management	4.7	1.0	1.0	1.3	4.2	1.0	4.5	4.2	2.8	1.0	4.8	4.2	1.0	3.8	4.4	1.5	2.1	1.0
Reporting Capabilities	3.3	3.5	4.1	3.8	3.0	4.2	3.2	4.6	4.2	4.3	4.7	3.6	3.1	3.6	4.9	3.3	3.0	4.9

Shared Device/Kiosk Management	4.8	1.0	1.0	1.0	3.0	3.6	4.3	4.4	2.9	1.0	4.4	4.3	1.0	3.6	4.5	1.5	3.5	1.0
Remote Support and Control	3.8	2.0	1.8	2.7	1.1	2.8	3.2	3.4	2.1	3.5	3.5	2.3	3.3	4.1	4.5	2.8	1.4	2.4
As of 5 December 2025																		

Source: Gartner (January 2026)

Table 3: Product Score in Use Cases

Use Cases	*42Gears*	*Absolute Security*	*Adaptiva*	*Atera*	*Google*	*HCLSoftware*	*IBM*	*Ivanti*	*Jamf*	*Kaseya*	*ManageEngine*	*Microsoft*	*N-able*	*NinjaOne*	*Omnissa*	*Raynet*	*Samsung Electronics*	*Tanium*
Unified Endpoint Management	3.61	1.86	2.06	1.50	2.90	2.80	3.53	4.14	2.68	1.30	4.10	3.79	1.72	3.37	4.29	1.90	2.62	2.21
Autonomous Endpoint Management	2.24	2.93	3.73	3.58	1.47	4.21	3.50	4.48	3.58	3.26	4.40	2.54	4.15	4.19	4.95	1.59	1.90	4.50
Security-Centric Management	3.15	3.21	3.76	3.46	2.68	3.80	3.71	4.23	3.48	3.72	4.36	3.46	3.80	4.01	4.80	2.38	2.45	4.39
Frontline Device Management	3.71	1.93	2.32	2.11	2.68	3.28	3.78	4.30	2.89	2.10	4.25	3.79	2.37	3.69	4.61	1.95	2.63	2.76

As of 5 December 2025

Source: Gartner (January 2026)