

Unified Endpoint Management (UEM) 2023

Richard Hill

May 30, 2023



**LEADERSHIP
COMPASS
2023**

This report provides an updated overview of the Unified Endpoint Management (UEM) market and provides a compass to help you find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing UEM solutions.

Contents

This report provides an updated overview of the Unified Endpoint Management (UEM) market and provides a compass to help you find the solution that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing UEM solutions.

Contents.....	2
Figures	3
Introduction / Executive Summary	3
Market Segment	5
Delivery Models	7
Required Capabilities	7
Leadership	9
Overall Leadership.....	10
Product Leadership.....	11
Innovation Leadership.....	13
Market Leadership	15
Correlated View.....	17
The Market/Product Matrix.....	18
The Product/Innovation Matrix	19
The Innovation/Market Matrix.....	20
Products and Vendors at a Glance	21
Product/Vendor evaluation	23
Aagon – Aagon Client Management Platform (ACMP).....	25
baramundi – baramundi Management Suite	28
Entgra – Entgra Suite.....	31
Hexnode – Hexnode UEM	34
IBM – MaaS360	37
Ivanti – Ivanti Neurons for UEM Premium with Security	40
Jamf – Jamf Suite	43
ManageEngine – ManageEngine Endpoint Central.....	46

Microsoft – Microsoft Intune	49
Miradore – Miradore.....	52
OpenText (Micro Focus) – ZENworks Suite	55
KACE by Quest.....	58
Sophos – Sophos Central	61
VMware – VMware Workspace ONE	64
Vendors to Watch.....	67
Methodology.....	69
Types of Leadership	69
Product rating	70
Vendor rating	72
Rating scale for products and vendors.....	72
Inclusion and exclusion of vendors	74

Figures

Figure 1: Unified Endpoint Management	5
Figure 2: The Overall Leadership rating for the Unified Endpoint Management market segment	10
Figure 3: Product Leaders in the Unified Endpoint Management market segment.....	11
Figure 4: Innovation Leaders in the Unified Endpoint Management market segment.....	13
Figure 5: Market Leaders in the Unified Endpoint Management market segment	15
Figure 6: The Market/Product Matrix	18
Figure 7: The Product/Innovation Matrix.....	19
Figure 8: The Innovation/Market Matrix	20

Introduction / Executive Summary

The landscape of enterprise and personal computing technology is continuously evolving. It does not seem that long ago that the work environment consisted of desktop computers and landline phones. Traditional management of desktop computers at the time relied on manual software updates and patches layered on top of each other. Later, “Gold Images” of desktop operating systems were used to provide a good, known state of the operating system (OS) but still required patches on a routine schedule, which would become what was known as traditional endpoint management.

As mobile phones became economically available, laptops and tablet computers replaced many stationary desktop computers; the business could control the employee device regarding its OS, the software applications used, and the security controls when the device was within the organization's perimeter. Client management tools were used to manage these environments. Client management involves capabilities such as OS deployment, software distribution, patch management, monitoring, and remote-control tools to support administration or to help automate other support functions that are typically executed manually.

Later, organizations needed to quickly deal with the introduction of the bring-your-own-device (BYOD) paradigm shift. Organizations required policies that defined the boundaries of BYOD, including the ability to segregate business data and applications from personal data and applications. Mobile device management (MDM) provides the tools to control the device functionality and help manage the lifecycle of these mobile devices and their platforms. Enterprise Mobility Management (EMM) solutions added mobile information, as well as application and content management. The ability to push software, updates, or patches to devices has become what is known as modern endpoint management.

Since then, work environments have continued to change. The range of endpoint device types has expanded past desktops, laptops, tablets, and mobile phones. Now endpoint types include printers, IoT devices, wearables like Apple Watch, and, more recently, endpoint devices that support virtual/augmented/mixed reality environments using headsets such as Oculus and HoloLens. Businesses seek to improve productivity and efficiency, while employees want to work-from-anywhere (WFA) at any time. And as we've seen with the Covid-19 world today, the ability to work from home is still imperative, requiring endpoint devices to access enterprise applications and data as if they were in the office. Given the WFA workforce paradigm, employees' experience interacting with their virtual workplace that utilizes endpoint applications, software, and other online tools must also be considered and supported.

With the complexity and growing number of technologies involved in linking employees to corporate data on-premises and in the cloud, mobile device management has undergone several iterations and approaches. Many enterprises are now standardizing on a Unified Endpoint Management (UEM) approach.

This KuppingerCole Leadership Compass provides an updated overview of vendors and their product or service offerings in the UEM market, ranging from vendors within more localized geographic regions to vendors with a global presence. The report also considers these services in the context of the hybrid, on-premises, and cloud, with IT service delivery models commonly found now in enterprise environments.

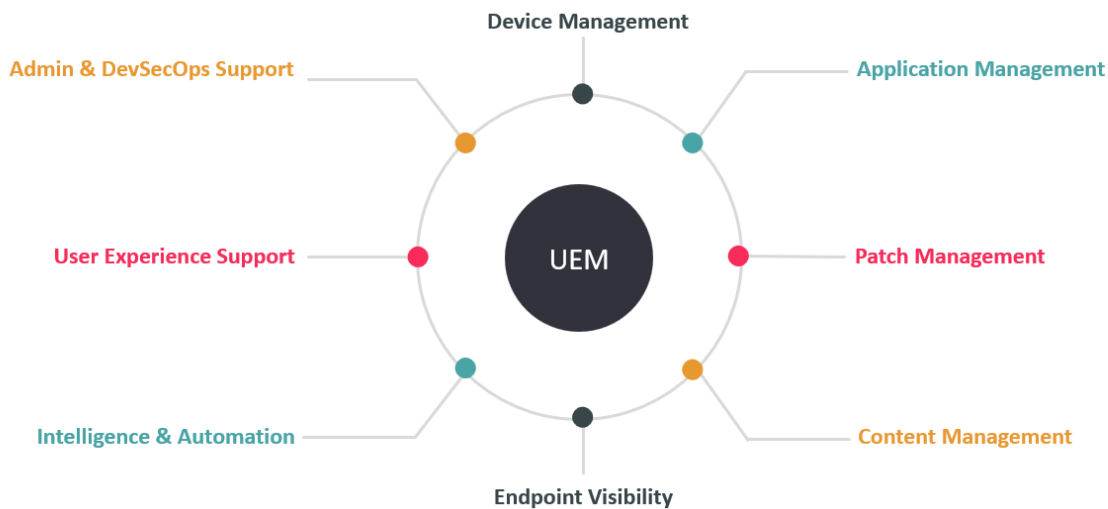


Figure 1: Unified Endpoint Management

Highlights

- The UEM market continues to evolve, adding innovative user experience capabilities to support the Work-From-Anywhere workforce.
- UEM continues to be essential to business as a strategic approach to ensure overall IT security in a hybrid work environment.
- The level of endpoint intelligence and automation is a key differentiator between UEM product solutions.
- Patch Management is one of the strongest capabilities for the majority of products evaluated in this Leadership Compass.
- Varying levels of Device and Application Management appear as differentiators between UEM product solutions.
- The Overall Leaders (in alphabetical order) IBM, Ivanti, Jamf, ManageEngine, Microsoft, KACE by Quest, VMware
- The Product Leaders (in alphabetical order) are Entgra, IBM, Ivanti, Jamf, ManageEngine, Microsoft, KACE by Quest, VMware
- The Innovation Leaders (in alphabetical order) are Entgra, IBM, Ivanti, Jamf, ManageEngine, Microsoft, VMware
- Leading vendors in innovation and market (a.k.a. the "Big Ones") in the UEM market are (in alphabetical order) IBM, Ivanti, Jamf, ManageEngine, Microsoft, VMware

Market Segment

Endpoint Management is a market category that runs under various names, such as Client Lifecycle Management, Enterprise Mobility Management, Unified Endpoint Management, and others. However, we see a clear trend toward comprehensive solutions supporting a variety of capabilities and types of endpoints. Thus, this Leadership Compass focuses on what is commonly referred to as Unified Endpoint Management. In this context, endpoints can be defined as traditional desktop or laptop computers, smartphones, tablets, wearables, printers, Point of Sale Kiosks, Internet of Things (IoT) devices, and even Virtual Reality (VR) headsets.

What is sometimes called client or service management involves capabilities such as OS deployment, software distribution, patch management, monitoring, and remote-control tools to support administration or to help automate other support functions that are typically executed manually. This type of management is also used to manage endpoint lifecycle, such as with UEM application management. Client management is a market segment in transition, as Unified Endpoint Management and Workspace Management have become the two major trends in client management.

The trend in recent years is the deprecation of classic client management, which usually focuses on Windows systems and the sole management of mobile endpoint devices (EMM, Enterprise Mobility Management). Most of the leading endpoint management providers today are focusing on Unified Endpoint Management. UEM solutions encompass the management of a wide range of endpoint device types and various operating systems such as Windows, macOS, Linux, or Chrome, as well as mobile endpoint devices with Android or iOS as the operating systems.

The range of functions such solutions offer goes far beyond classic client management. It also includes the provisioning of configured work environments for employees, inventory, and management of the operating system and applications, but also the management of content on end devices, for example, the separation of personal and business apps and data.

Patch management, which in the past was offered more often as a separate product category, is now an integral part of UEM solutions. Also, Endpoint security capabilities can be included in UEM solutions, which sometimes intersect with other Endpoint Detection & Response (EDR) products. More information on this topic can be found in the KuppingerCole Buyer's Compass: Endpoint Detection & Response (EDR).

The shift toward a Work-From-Anywhere (WFA) workforce has increased the importance of monitoring user interactions with their digital workplace to improve the employee experience. Organizations can proactively discover and remediate issues to reduce user friction and improve their overall experience by monitoring user interactions with their device, applications, and other services. This also has the added benefit of reducing the load on the IT help desk. Solutions to address this exist in different markets, such as Digital Employee Experience (DEX), End-User Experience Management (EUEM), and Digital Experience Monitoring (DEM). This Leadership Compass will evaluate a UEM's ability to support user experience as an innovative capability in the UEM market.

In addition to these influencing factors of workspace and user device expectations, other factors need to be considered when deciding how endpoint management will continue to be designed in the future. These include changes in application provisioning, endpoint management from the cloud, managing cloud endpoints, integration with ITSM (IT Service Management) solutions, and the different concepts for endpoint management on the one hand and for the provision of virtual work environments, i.e., the Digital Workspaces, on the other.

Here are some considerations of UEM solutions that this Leadership Compass covers:

- Products that are more classic software solutions that are installed and operated locally.
- Cloud and hybrid UEM solutions

- Providers that have options for operation "as a service" that allow complete UEM to be obtained as a service without the need to install and operate servers locally.
- The areas of UEM that the solution focuses on (e.g., device, application, security, patching, etc.)
- The breadth of operating systems and device types that the solution can support.
- The depth of endpoint life cycle management the solution provides.
- The level of application software, packaging and patch management provided.
- Solutions that provide endpoint content management and containment capabilities
- The level of intelligence and automation used within the UEM solution.
- The level of admin and DevSecOps support is given.
- The level of user experience support that the UEM solution provides.

Ultimately, the selection of any UEM solution on the market will depend on the organization's particular requirements, which may depend on many other aspects, such as existing infrastructure management or other IT solutions currently being used today. For example, if a specialized endpoint security solution is already in use, this functional area of UEM solutions is less or not at all relevant. Or, if the organization only needs to focus on device and patch management capabilities, then maybe some fully featured UEM solutions may not be required, and a UEM solution with those specific features may be a better fit. In all cases, it is recommended that a structured selection process should be carried out before the product decision is made.

Delivery Models

Although all delivery models are looked at, it is worth considering the pros and cons of each delivery model. For instance, it is good to be aware that public cloud solutions are generally multi-tenant in most cases, while some cloud services are single tenant. Other approaches use container-based deployments to deliver a vendor's cloud-hosted or on-premises solution consistently. Ultimately, selecting a suitable Unified Endpoint Management solution delivery model will depend on the customer requirements and use cases.

Required Capabilities

This Leadership Compass analyses the main attributes and functions of Unified Endpoint Management solutions. At a high level, these capabilities should include some level of:

- Endpoint life cycle management
- Application management
- Patch Management
- Endpoint security
- Endpoint content management
- Endpoint visibility

- Endpoint intelligence
- Automation of tasks that would normally be done manually.
- Administration and DevSecOps support

Drilling down a little deeper for each of the high-level UEM capabilities above, here are some of the capabilities considered:

Endpoint Life Cycle Management:

- Endpoint onboarding
- Provisioning
- Decommissioning
- Remote access or wiping
- Inventorying
- OS management

Application Management:

- Applying policies and controls to applications on the endpoint
- Application whitelisting and/or blacklisting applications
- Support for bulk distributions of applications or configurations
- Application packaging
- Enterprise App Store enrollment of users and their devices

Patch Management:

- Distribute & apply endpoint device system patches from various vendors
- Patch deployment on a schedule or critical/emergency patches
- Reporting of endpoint system status (e.g., patch level)
- Missing patch discovery e.g., security hotfix, application, or others
- Patch vulnerability testing
- Some level of patch automation

Endpoint Content Management:

- Ability to separate business from personal apps and data
- Prevent sensitive data leaks
- Apply rules and policies to documents and other content on the device
- Audit trails for device configuration changes and access to sensitive content

Endpoint Intelligence:

- Some level of analytics and/or AI/ML to provide endpoint insight
- Analytics to detect risks based on user, app, and/or endpoint behavioral patterns
- Ability to smartly assist or take action to remediate endpoint related issues
- Make recommendations based on endpoint state, security posture, etc.

Endpoint Security:

- Authentication
- Access policies
- Context-based access
- Certificate management
- Security alerts
- Application code signing
- Enforcement of endpoint least privilege or EPM integration
- Integrations with IAM and/or other products such as EDR

Administration and DevOps Support:

- Solution deployment and delivery models
- Available APIs, CLIs, SDKs, etc.
- Standards support
- Compliance support
- User and admin UIs, dashboards, centralized endpoint visibility
- Reporting
- Developer portal or other product documentation, tutorials, examples, etc.
- Integration options (ITSM, SIEM, third-party extensions, etc.)
- Level of automation

Innovative Capabilities:

- Endpoint Discovery
- User Experience Support (i.e., DEX, DEM, EUEM)
- IoT, virtual/mixed reality glasses, server, and cloud infrastructure endpoint support
- Endpoint troubleshooting via analytics and intelligence
- Automated Endpoint Remediation
- Endpoint Life Cycle, Patch, and/or Content Management intelligence
- Intelligent insight into user and/or device behavior
- Intelligent insight into user and/or device risk level
- Ability to make recommendations regarding endpoint improvements or efficiencies
- Automation (e.g., automate common admin tasks, deployment automation, etc.)
- Support for Admin and DevOps automation tools
- Shift left support for software packaging before deployment.
- Modern architectures

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identifying vendors that shall be

further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

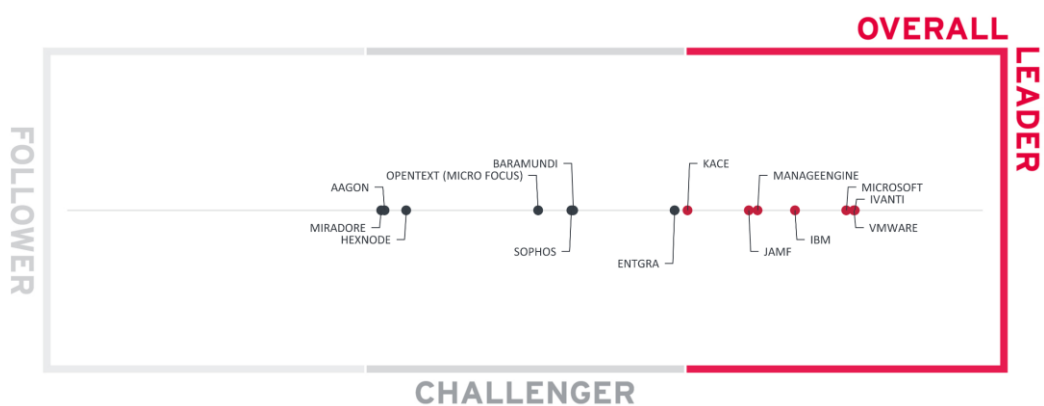


Figure 2: The Overall Leadership rating for the Unified Endpoint Management market segment

Overall Leaders are (in alphabetical order):

- IBM
- Ivanti
- Jamf
- ManageEngine
- Microsoft
- KACE by Quest
- VMware

Product Leadership

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of service features and the overall capabilities of the various services.



Figure 3: Product Leaders in the Unified Endpoint Management market segment

Product Leadership, or in this case Service Leadership, is where we examine the functional strength and completeness of services.

Product Leaders (in alphabetical order):

- Entgra
- IBM
- Ivanti

- Jamf
- ManageEngine
- Microsoft
- KACE by Quest
- VMware

Innovation Leadership

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

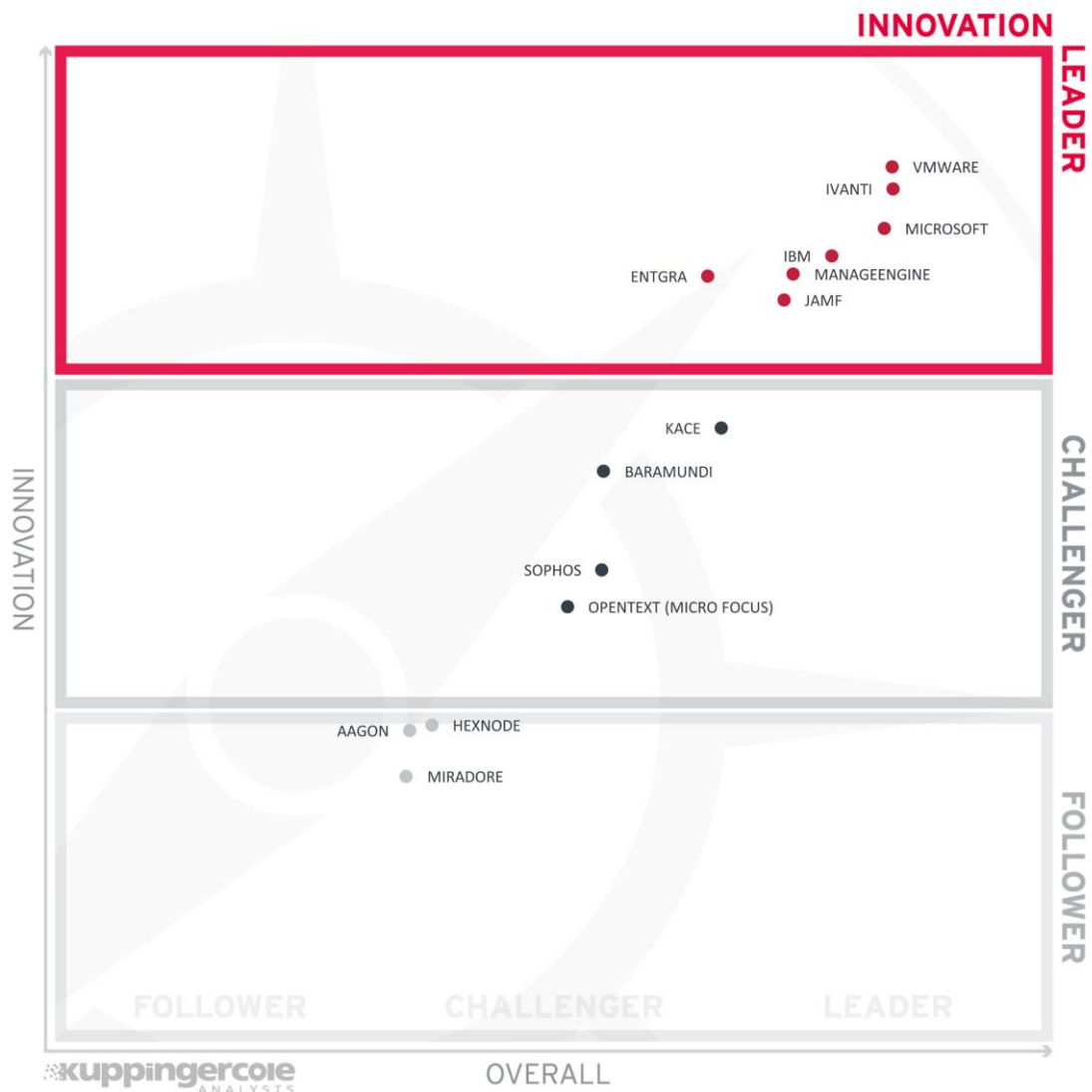


Figure 4: Innovation Leaders in the Unified Endpoint Management market segment

Innovation Leaders (in alphabetical order):

- Entgra
- IBM

- Ivanti
- Jamf
- ManageEngine
- Microsoft
- VMware

Market Leadership

Lastly, we analyze **Market Leadership**. This is an amalgamation of the number of customers, number of transactions evaluated, ratio between customers and managed identities/devices, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and financial health of the participating companies. Market Leadership, from our point of view, requires global reach.



Figure 5: Market Leaders in the Unified Endpoint Management market segment

Market Leaders (in alphabetical order):

- IBM
- Ivanti
- Jamf

- ManageEngine
- Microsoft
- KACE by Quest
- VMware

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The first of these correlated views contrasts Product Leadership and Market Leadership.

The Market/Product Matrix

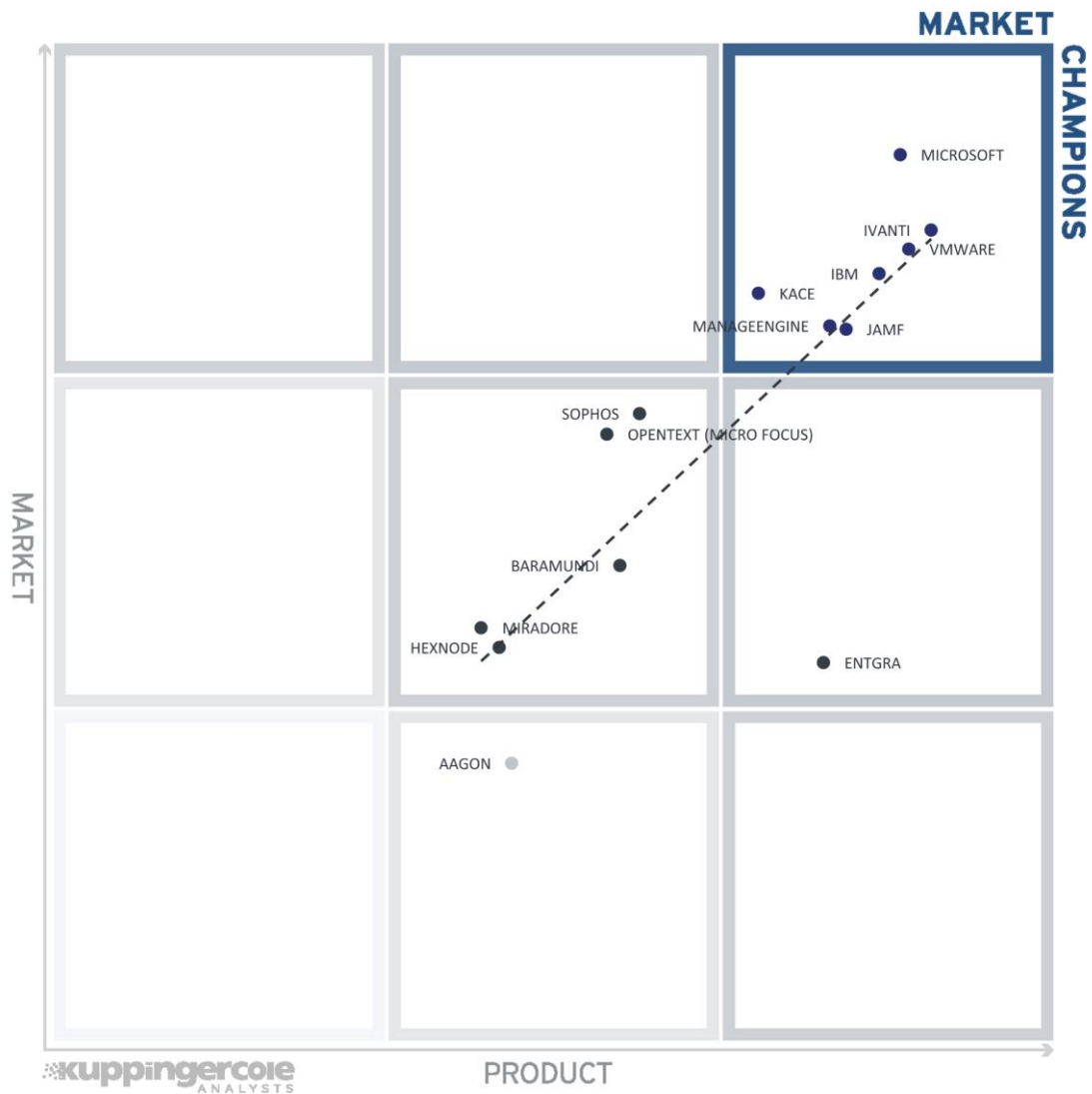


Figure 6: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a considerable number of established vendors plus some smaller vendors.

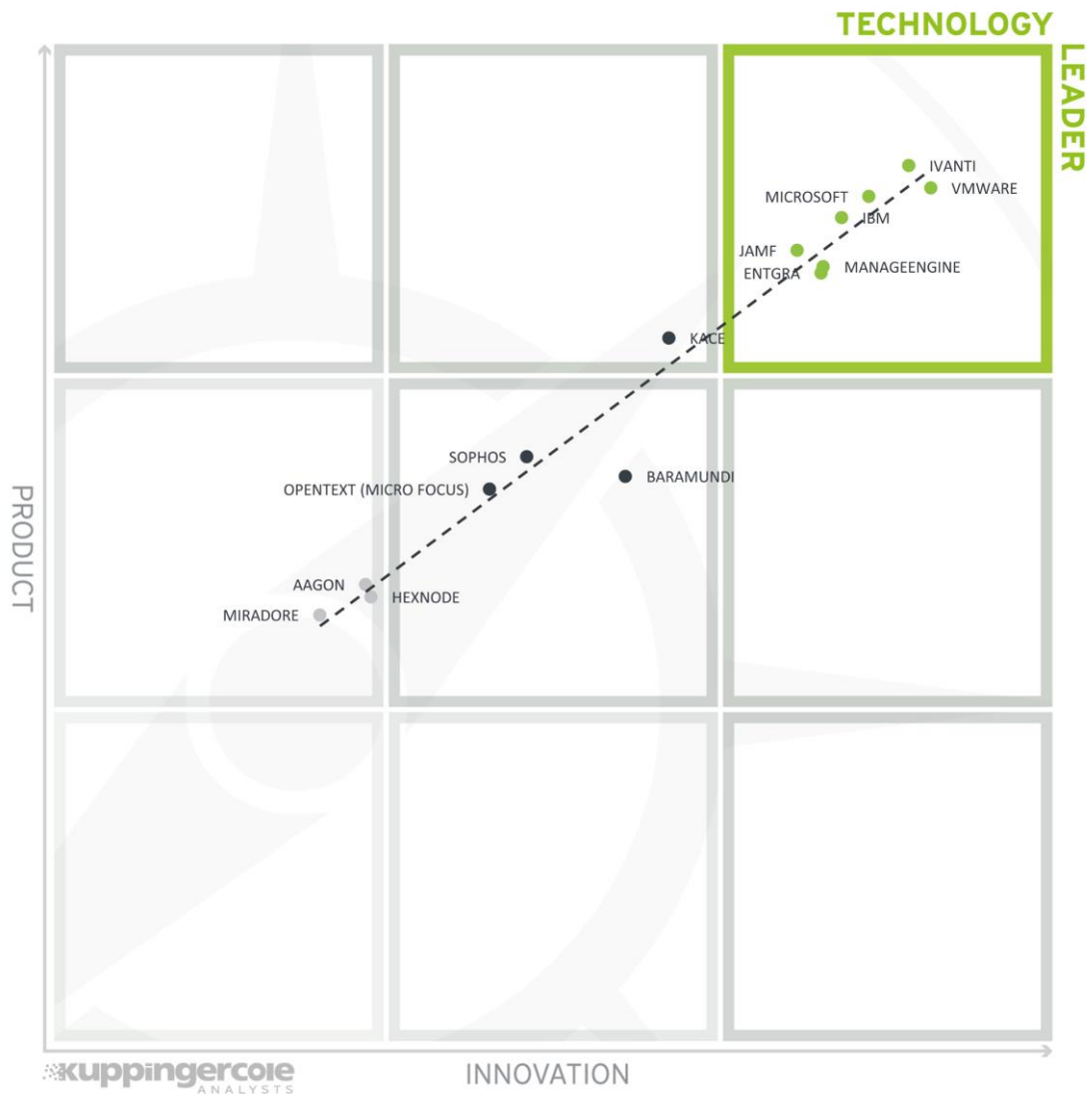


Figure 7: The Product/Innovation Matrix

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

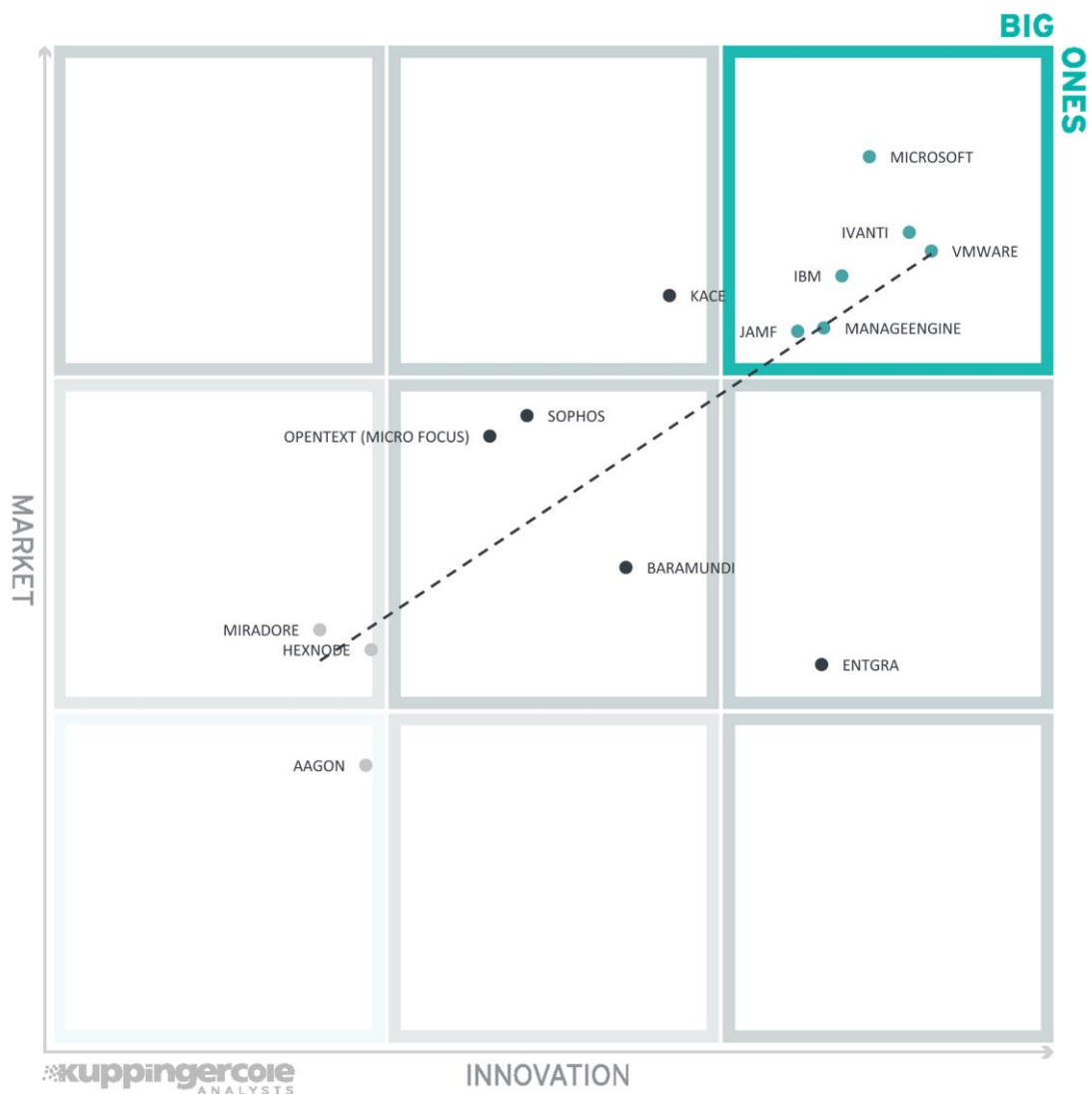


Figure 8: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Fraud Reduction Intelligence Platforms. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name

Product(s) from Vendor	Security	Functionality	Deployment	Interoperability	Usability
AAGON	Neutral	Neutral	Neutral	Neutral	Neutral
BARAMUNDI	Neutral	Positive	Neutral	Positive	Positive
ENTGRA	Strong Positive	Strong Positive	Positive	Positive	Positive
HEXNODE	Neutral	Neutral	Neutral	Neutral	Neutral
IBM	Strong Positive	Positive	Positive	Strong Positive	Strong Positive
IVANTI	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
JAMF	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
MANAGEENGINE	Strong Positive	Strong Positive	Positive	Positive	Strong Positive
MICROSOFT	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
MIRADORE	Neutral	Weak	Neutral	Neutral	Neutral
OPENTEXT (MICRO FOCUS)	Positive	Positive	Positive	Neutral	Positive
KACE BY QUEST	Positive	Positive	Positive	Positive	Positive
SOPHOS	Positive	Neutral	Neutral	Positive	Positive
VMWARE	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
AAGON	Critical	Neutral	Positive	Weak
BARAMUNDI	Neutral	Neutral	Positive	Neutral
ENTGRA	Positive	Weak	Neutral	Weak
HEXNODE	Critical	Neutral	Neutral	Neutral
IBM	Positive	Positive	Strong Positive	Positive
IVANTI	Strong Positive	Positive	Positive	Strong Positive
JAMF	Positive	Positive	Positive	Positive
MANAGEENGINE	Positive	Positive	Positive	Positive
MICROSOFT	Positive	Strong Positive	Strong Positive	Strong Positive
MIRADORE	Critical	Neutral	Neutral	Neutral
OPENTEXT (MICRO FOCUS)	Weak	Positive	Positive	Positive
KACE BY QUEST	Positive	Positive	Positive	Positive
SOPHOS	Weak	Positive	Positive	Positive
VMWARE	Strong Positive	Positive	Strong Positive	Positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we have included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the LC Unified Endpoint Management, we look at the following six categories:

- **Device Management**- Management of various endpoint device types, which includes its life cycle management, such as onboarding, provisioning, decommissioning, operating system management, remote access for support, troubleshooting or wiping, and device inventory.
- **Application Management** - This category focuses on the ability to control and apply policies to applications regarding endpoint devices and other application management features. It can include the capability to enroll devices and users via App Stores, software packaging and deployment, distribute applications to endpoints, whether bulk or otherwise, apply aspects of security such as white or blacklisting applications, isolate corporate from private user applications, etc.
- **Patch Management** - This category focuses on the ability to distribute and apply endpoint device system patches (e.g., OS, application, etc.) from various vendors, whether the patch is deployed on a schedule or critical/emergency patches are distributed rapidly when necessary. Some other capabilities include reporting endpoint system status (e.g., patch level), missing patch discovery whether it is a security hotfix, application, or others, level of automation, etc.
- **Content Management** - Endpoint content management refers to the ability to apply access rules and policies to documents or other content on the endpoint device. The rules and policies can be coarse or fine-grained enough to apply to an individual file. Capabilities can also include catalogs of enterprise documents, content security, as well as audit logging, etc.
- **Endpoint Visibility** - The ability to provide a consolidated view and management of all endpoints regardless of where the solution is deployed. Endpoint visibility often features a single pane view via a dashboard and provides visibility to device inventory, state, threats, policy management, licenses, reporting, etc.
- **Intelligence & Automation** - This category looks at the level and use of analytics and/or artificial intelligence to provide insight into different aspects of the UEM domain as well as the ability to automate, assist or take action to remediate endpoint-related issues, as well as other capabilities.
- **User Experience Support** - The ability to support the collecting and monitoring of end-user devices, applications, and activity information for the purpose of improving the end-user experience. This can include benchmarking workforce experience against

internal goals, correlating a user's experience with other data sources, providing automation and remediation capabilities to proactively reduce the friction of end-user issues with their device or application, reporting on end-user experience, or even the ability to integrate with other third-party or partner products that can provide this capability to the UEM product.

- Admin & DevSecOps Support - The ability to provide support options for administrators of the UEM solution, IT security, and the operations team regarding their tools, automation, and continuous integrations.

Aagon – Aagon Client Management Platform (ACMP)

Aagon Client Management Platform (ACMP) provides a fully integrated and comprehensive solution for distributing and patching software with advanced automation features and is data protection compliant. Founded in 1992, Aagon is a German company based in Soest with offices in Berlin and Munich. Aagon has over 30 years of Client Management experience with customers primarily focused in the DACH region, with increased growth in North America and APAC.

The Aagon Client Management Platform is modular, providing flexible endpoint device, patch, license, asset, contract, and compliance management. ACMP also offers integrated service desk and hardware asset management, endpoint discovery, vulnerability detection & remediation, and security capabilities. Traditional endpoint types are supported, which provides support for desktops, laptops, tablets, smartphones, servers, printers, and SNMP scanning devices. Supported endpoint operating systems include iOS, Android, Windows, macOS, and Linux. Chrome OS is not supported.

ACMP provides complete endpoint lifecycle management, such as automated user onboarding and provisioning devices and applications that its client commands can customize. Endpoint activation, decommissioning, and remote access with device locking and wiping capabilities are also available. Aagon shows a particular strength with patch management, supporting Windows, macOS, and Linux operating systems and the ability to scan & detect endpoint software such as versions, patch-level, and device health. Windows update management has also been added. Application software deployment and packaging include creating and customizing software packages. The solution can also apply policies and controls to applications on the endpoint. Application whitelisting and blacklisting is not available. The integration and control of the Microsoft Defender management and BitLocker management are newly offered. The ACMP provides a familiar and detailed UI for managing its capabilities.

ACMP is partially implemented as in microservices providing a more modern architecture. The solution includes agent software installed on endpoint devices for functionality that handles all software installations, whether updates, software installations, or the completion of administrative tasks. The Agent can also provide self-service kiosk functionality. Aagon provides ACMP for on-premises deployments and can deliver ACMP as either software to servers, a virtual appliance, or as a managed service and SaaS provided through Aagon's partners. Cloud and container-based options are currently not available. For the on-premises deployment, a Microsoft SQL Server is required. Over half of the ACMP functionality is accessible via SOAP, REST, JSON-RPC, XML-RPC, Webhooks, or PowerShell APIs. Aagon intends to increase ACMP functionality via API with each product release. Integrating third-party solutions such as ITAM, ITSM, threat intelligence, EDR, EPP, AI/ML, or analytics is possible over Public APIs. Access to ACMP functionality via CLI or SDKs is not available. A developer portal is on Aagon's near-term roadmap, targeted for the first half of 2023.

Aagon offers a viable solution for companies in the DACH region requiring endpoint device, application, and patch management capabilities. Aagon customers are primarily medium to

mid-market organizations that can meet the needs of both small and enterprise companies and a good partner ecosystem.

Security	Neutral	
Functionality	Neutral	
Deployment	Neutral	
Interoperability	Neutral	
Usability	Neutral	

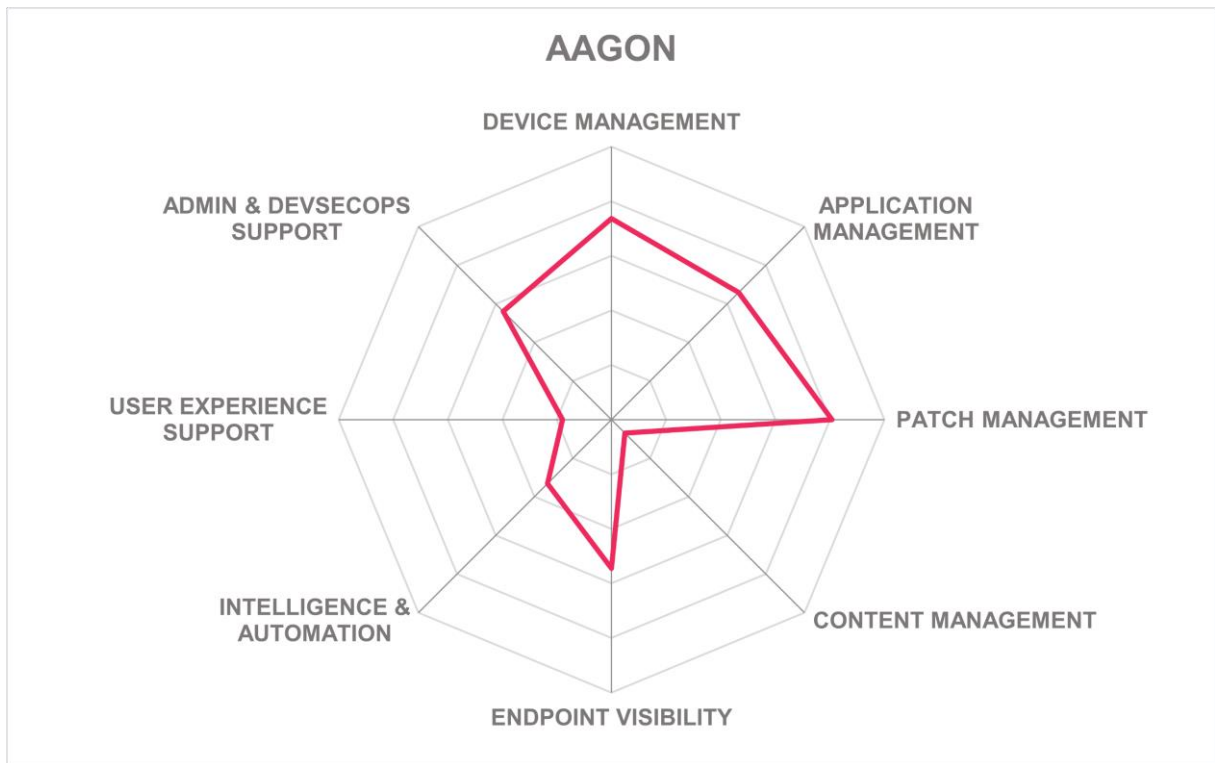
Table 3: Aagon's rating

Strengths

- Patch management
- Device management
- Application management
- Admin and DevSecOps support
- Endpoint visibility
- Automation capabilities
- Compliance management support

Challenges

- Primarily focused on the DACH region with limited global reach
- Chrome OS is not supported
- Missing content management
- Limited endpoint intelligence
- Minimal user experience support
- Missing cloud deployment option without Aagon's partners



baramundi – baramundi Management Suite

Founded in 2000 and headquartered in Augsburg, Germany, with branch offices in Austria and USA. baramundi software AG is owned by Wittenstein SE, Germany. The baramundi Management Suite focuses on securing cross-platform management of workstations and other endpoint environments focused on transparency through discovery, analytics, user focus, and performance, such as faster packaging and the ability to customize commands assigned to endpoints.

The baramundi Management Suite supports mobile endpoint, application, and content management, with patch management as one of its strongest capabilities. Also, management of assets, licenses, and contract management is supported, among other features. Device provisioning, health monitoring, and location tracking are also given. A good range of endpoint devices can be supported, which includes traditional and mobile devices, printers, wearables, IoT devices, Point of Sale Kiosks, and servers. It also uniquely extends to SNMP devices, SIEMENS Simatic (PLCs), and Rugged Android Mobile Devices (e.g., CipherLab). Endpoint operating system support includes iOS, Android, macOS, and Windows, although it is missing Linux and chrome support.

The baramundi Management Suite endpoint lifecycle management provides customizable and automated device and application onboarding utilizing Apple DEP, Android Work Profile, and Microsoft Autopilot. It uses a push-based paradigm and supports the scripting of endpoint life cycle management tasks. The solution gives good endpoint discovery capabilities with hardware and software information and analyzes discovered endpoints for vulnerabilities and compliance. Remote troubleshooting of endpoint devices is also supported. The platform provides strong patch management support for iOS, Android, and Windows, although macOS, Linux, and Chrome are not supported. For Android, only updates of applications are supported, while system updates are not. The baramundi Management Suite provides a tab-based UI with administrative dashboards, endpoint views, preconfigured tasks, and client custom commands as some examples. The product is GDPR certified, although predefined compliance reports, such as GDPR, HIPPA, or PSD2, are not provided. Innovative is baramundi's End User Experience Management (EUEM) capabilities provide insights into issues or problems with an endpoint from the point of view of the end user, giving the administrators of the solution the opportunities to remediate them before ITSM tickets arise.

The product is implemented with a microservices architecture and supports on-premises, cloud, and hybrid deployment models. It can be delivered as a virtual appliance or software deployed to a server. A managed service is available through partner organizations, including software packaging for installing and updating managed software. REST and JSON RPC APIs are available to access the solution's capabilities. Although access to the solution's capabilities via CLI or SDKs is limited, although they do provide its bConnect 1.1 interface that enables scripting and a recently released API called bConnect 2.0 based on openAPI. Good third-party integration support is given, such as ITSM, Threat Intelligence, EPP, EDR, DEX, and EUEM solutions, as some examples. A customer and partner portal are available with documentation, tutorials, and examples to help with development, integrations, configuration, and deployments.

baramundi Software is a privately-owned company serving the SMB market with a strong EMEA regional presence and a growing presence in North America. baramundi Software shows strengths in the device, application, patch management areas, and some innovative EUEM capabilities. Overall, baramundi continues to improve its UEM solution and provides a comprehensive set of UEM capabilities.

Security	Neutral	
Functionality	Positive	
Deployment	Neutral	
Interoperability	Positive	
Usability	Positive	

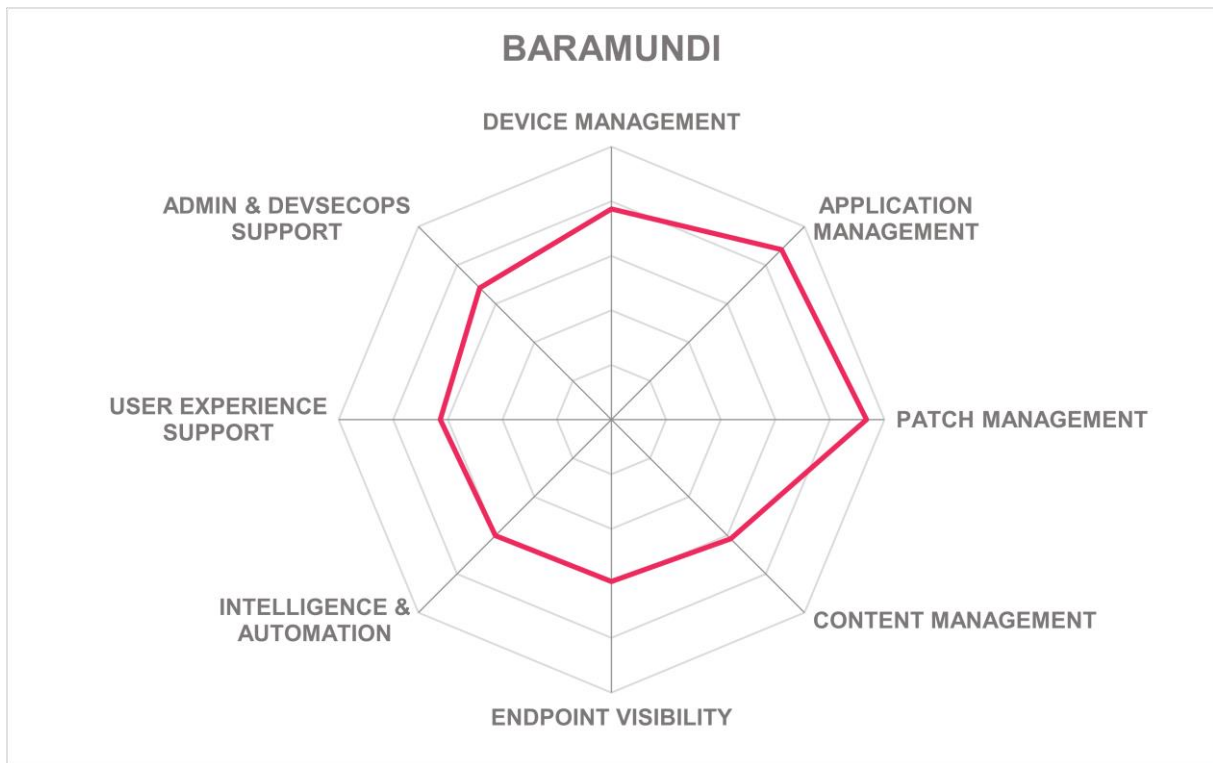
Table 4: baramundi's rating

Strengths

- Strong Patch management
- Application management
- Device management
- EUEM capabilities
- Content management
- Endpoint visibility
- Admin & DevSecOps support
- Good and unique range of endpoint devices support
- Support for industrial device and controls use cases

Challenges

- Primarily centered on the EU with limited global reach
- Relatively small partner ecosystem outside of the EMEA region, although growing in NA
- Missing support for Linux, and Chrome endpoints, although Linux support is on its near-term road map with an expected release later this year
- Limited CLI and SDK support, but does provide its bConnect 1.1 scripting interface and its bConnect 2.0 API



Entgra – Entgra Suite

Entgra is a single platform with multiple products for enterprise Internet of Things (IoT), Unified Endpoint Management (UEM) & Enterprise Mobility Management (EMM) needs. Entgra started as a WSO2 vertical called the Device Integration Platform and later spun out of WSO2 in 2018. Today, Entgra maintains the OEM license to embed WSO2 technologies and is a technology partner for all WSO2 IoT and MDM customers. The Entgra offerings considered in this UEM Leadership Compass include Entgra IoT Server, Entgra Edge G/W, Entgra IoT Server (UEM Profile), and Entgra Smart Grid Middleware.

Entgra capabilities provide device, application, identity, content, patch, license, and asset management as a few examples. Also offered is device provisioning, health monitoring, and location tracking are also offered. Endpoint intelligence and analytics are also available, for example analytics are used to prevent attacks on APIs. Features such as Mobile Threat Defense (MTD) and Mobile Threat Defense (MTD) require integration with Kaspersky. Support for a wide range of endpoint device types includes desktops, laptops, smartphones, IoT, printers, smartboards, TV OS, mixed reality headsets, point-of-sale kiosks, and ATMs. More industrial use cases are also supported, such as SNMP devices, programmable logic controllers (PLC), smart utility meters, weather stations, and smart cameras, to name a few. More recently, wearables and virtual business assistants are also supported. Entgra also supports a wide range of endpoint operating systems such as iOS, Android, Windows, macOS, Linux, and Chrome, as well as FireOS, Android TVOS, FreeRTOS, Lua RT, and Micro Python RT.

One of Entgra suite's significant capabilities besides device management is patch management. Endpoint patch management covers iOS, Android, macOS, and Linux-based devices. Windows and Chrome patch management support are currently not supported. Entgra relies on external packaging tools or deployment pipelines to build software application packaging. The solution can then be configured to manage the remainder of the publishing workflow and delivery of the software application packages. Entgra provides a modern and useful UI with embedded analytics dashboards. The device fleet view includes tracking a device in a map view through its Complex Event Processor engine integration and extended Grafana dashboards. Also, all data used by dashboards and management consoles are available as API endpoints. Entgra supports user experience through monitoring endpoints, such as endpoint patching and OS deployments, which can be used to troubleshoot service degradation. All collected attributes and events are available as APIs for a 3rd party DEX solution to integrate with Entgra's platform and use.

Entgra platform can be deployed as software, hardware, or a virtual appliance on-premises, as well as a fully multitenant cloud SaaS service, hybrid, or managed service. Entgra is partially implemented as a microservice and supports its product delivery as Docker containers which can be deployed to container-orchestration systems such as Kubernetes. Entgra's capabilities are accessible via SOAP, REST, and Webhook APIs. WebSockets support and MQTT for event publishing are also available. CLI is available for bulk enrollment and uploading of devices only, although curl commands are available to cover the full range of product APIs. Less access to product capabilities is given via SDKs, and support is available for Android, iOS, Java, C/C++, .NET, and Python programming languages, as

well as support for Arduino and Raspberry Pi. Support is also available for Nuvoton microcontrollers and ATxmega and Quectel microchip technologies. Agent software collects data from a device, executes commands from the server end, and executes localized policies. Also, support for custom agents can run on legacy hardware platforms and configure for specific endpoints, supporting legacy capabilities. The Entgra solution has also been independently certified to comply with the FIPS 197, FIPS 140-2, NIST 800-57 Key Management, IEC 60870-5-104, and IEC 62056 DLMS/COSEM standards.

Entgra’s platform uniquely supports IoT and Mobile Device Management use cases and leverages an already good IAM product by building on top of the WSO2 middleware stack. Entgra customers are medium-sized organizations focused in the APAC region, followed by EMEA and North American regions. Entgra continues to innovate and grow its market presence and leverages WSO2, which includes a good worldwide presence. For organizations requiring endpoint management beyond the traditional device types, Entgra offers an interesting alternative UEM solution.

Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

Table 5: Entgra’s rating

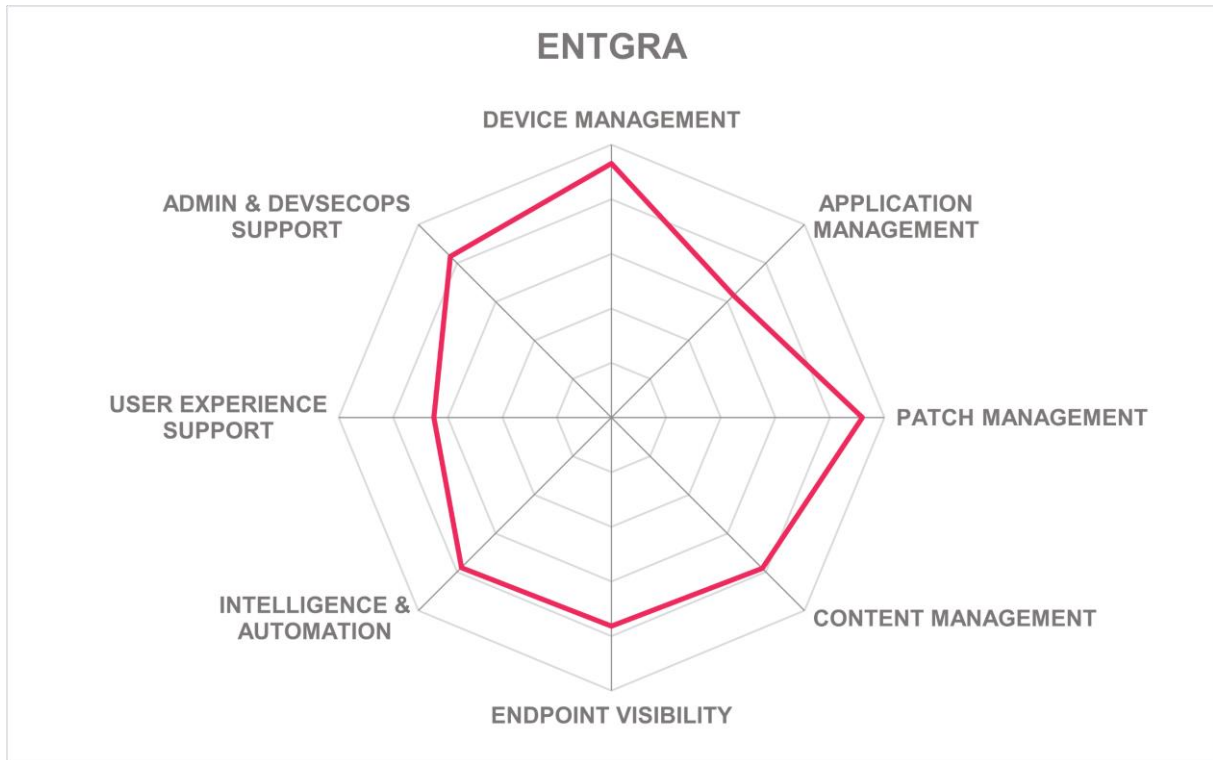
Strengths

- Strong patch management
- Good device management
- Content management
- Endpoint intelligence and automation
- Wide range of endpoint types supported
- Admin & DevSecOps support
- Centralized endpoint visibility
- User experience support

Challenges

- Limited marketing visibility
- Some application software packaging limitations
- Remote only customer support
- Missing Windows and Chrome patch management support
- Limited OOB integrations with third-party axillary solutions, although custom integration via REST APIs is possible

Leader in



Hexnode – Hexnode UEM

Founded in 2013 and headquartered in the San Francisco Bay area with offices in Atlanta, Australia, Germany, and India, Hexnode is a software division of Mitsogo Inc., which provides a single centralized platform for device, application, content, and identity for companies ranging from SMBs to the enterprise level.

Hexnode UEM product focuses on device, application, content, asset, and expense management. Device health monitoring and tracking are available, as well as endpoint security, vulnerability detection & remediation, endpoint detection and response (EDR), and threat defense. In addition, remote access management for remote troubleshooting is offered. Limited are more advanced capabilities, such as endpoint discovery and intelligence or analytic capabilities. More traditional endpoint devices such as desktops, laptops, tablets, smartphones, TV OS, point-of-sale kiosks, and industrial mobile devices are supported. Support for device types such as IoT, wearables, and smartboards has been recently added. Endpoint operating systems support includes iOS, Android, and Windows 10 and 11, with added macOS, FireOS, and tvOS support. Still, support for Linux or Chrome is yet to be offered. Support for ITAM, ITSM, EDR, EPP, and threat intelligence solutions have been added. However, integrations with third-party Analytics or Intelligence (AI/ML), endpoint discovery, DEX, and EUEM solutions are not.

Endpoint lifecycle management includes automated user onboarding, provisioning of users, devices, applications, content, and endpoint activation and decommissioning. An inventory of all endpoints is also given. Workflows have been implemented for device enrollment, app installation and management, device and user management, license management, device reassigning and unenrolling, and report generation. Support scripting of endpoint life cycle management tasks and remote troubleshooting of endpoints is given. Limited patch management capabilities are available, although endpoint health policy management with the ability to scan, detect, and report on the endpoint software version, patch level, and health are available. Hexnode can deploy applications such as a store, VPP, web, web clips, and enterprise apps. Hexnode application management can also upload the application files into the inventory and distribute them across devices. Admins can apply policies on Hexnode to configure applications for endpoint use. Options to Allowlist or Blocklist applications at the endpoint are also given. Endpoint containment and content management capabilities are given, separating business from personal apps and data. Containment policies can prevent users from copying, sharing, or even opening sensitive documents in unmanaged applications. Admins can implement policies on Hexnode to prevent data from being copied or transferred to external drives.

A web-based interface provides a good administrative dashboard as well as a simple and useful centralized UI with a view of analytics and intelligent insights into endpoints under management. Hexnode provides many out-of-the-box (OOB) reports, although they are not customizable. Hexnode UEM is delivered SaaS, which can be deployed to a private cloud environment. Most of the solutions, actions, and policies can be configured via REST APIs. Device, user, and application details can also be retrieved via APIs. CLI and SDK access to product functionality are not available. Hexnode's product has been independently certified to support compliance standards such as Privacy Shield Framework, GDPR and independently

audited to support compliance with ISO/IEC 27001 and is currently in the process of obtaining AICPA's SSAE 18 SOC 2 Type 2.

Hexnode has steadily increased its core UEM capabilities, although KuppingerCole would see patch management as a worthwhile improvement in Hexnode's product offering. Hexnode's customers are SMB to mid-market, with some presence in enterprise organizations in North America, EMEA, and the APAC regions. Small to mid-market organizations requiring UEM capabilities for endpoint devices, applications, and content management can evaluate Hexnode UEM.

Security	Neutral	
Functionality	Neutral	
Deployment	Neutral	
Interoperability	Neutral	
Usability	Neutral	

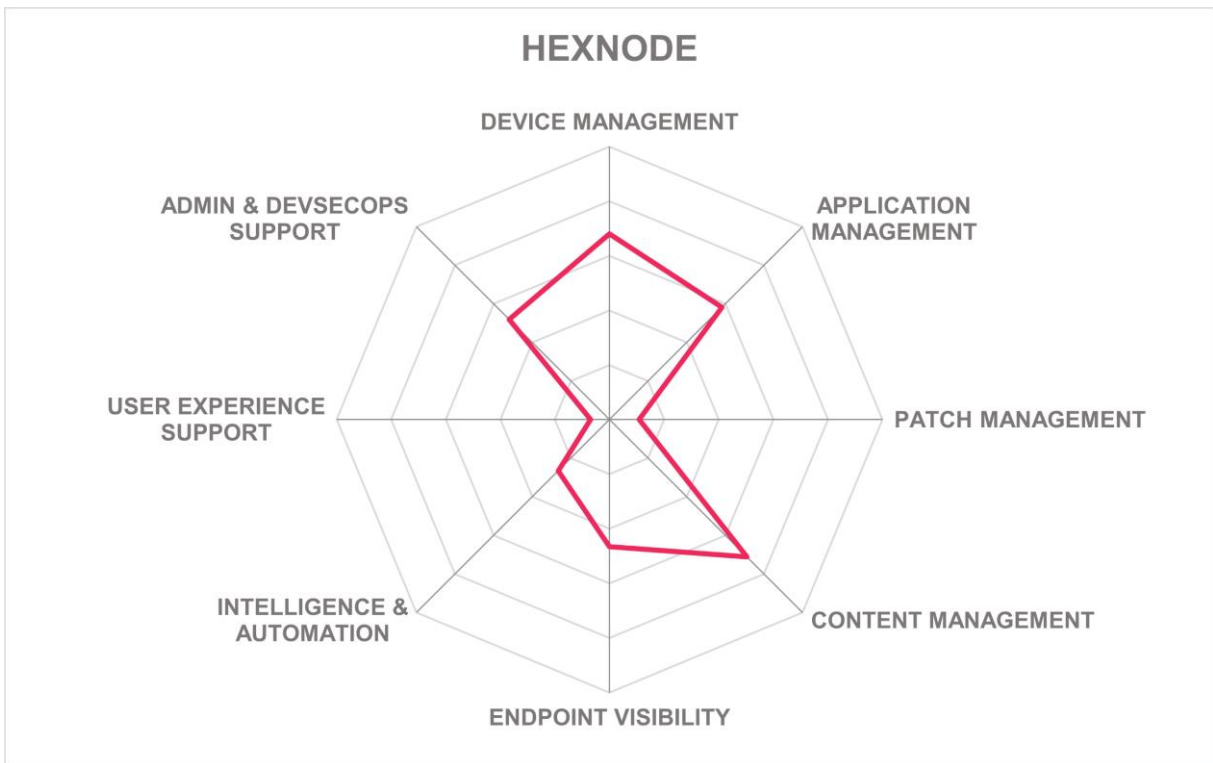
Table 6: Hexnode's rating

Strengths

- Device management
- Expanding support for endpoint device types and operating systems
- Content management
- Application management
- Endpoint visibility
- Moderate admin and DevSecOps support
- Ability to push and manage certificates onto the endpoint
- Administration MFA authentication options

Challenges

- Small, but growing partner ecosystem
- Missing support for Linux and Chrome OS
- Missing patch management
- Missing user experience support
- Missing CLI and SDK support
- Limited deployment options
- Limited endpoint intelligence and automation
- Limited API options beyond REST



IBM – MaaS360

IBM is one of the leading companies in IT. Founded in 1911, it is one of the largest US-based firms. IBM MaaS360 with Watson has since evolved from a traditional cloud-based endpoint management product to an AI-enabled software-as-a-service (SaaS) Unified Endpoint Management (UEM) platform designed to give enterprises the ability to manage and secure a wide range of devices.

IBM Security MaaS360 covers a wide range of UEM features, including endpoint devices, applications, content, patch, asset, license, expense management, endpoint security, device provisioning, tracking, and health monitoring. Advanced capabilities include containment (Secure PIM Suite), insider threat detection, and zero trust. Some Employee Experience (DEX) capabilities are also available. MaaS360 gives broad support of endpoint types beyond desktops, laptops, and mobile devices. Also supported are servers and wearables (e.g., Apple Watch). Most endpoint operating systems are supported, such as iOS, Android, Windows 10 & 11, macOS, Chrome, as well as FireOS, and LinkOS (Zebra Printer); however, Linux operating systems are not. Although IoT and business virtual assistants use cases are missing, mixed reality headsets and commerce point-of-sales, ATM, and industrial mobile devices are supported.

One strength is MaaS360 with Watson, which provides intelligence and remediation abilities that give actionable insights and contextual analytics to their UEM offering. MaaS360 provides good endpoint containment capabilities, which are accomplished through containerization, DLP, data separation on personal devices, and encrypted sandboxing. The MaaS360 Assistant, with AI capabilities embedded, allows it to perform NLP-based queries in the container. It can also provide threat and attack detection of contained apps or data, both natively embedded with IBM Trusteer as well as via partnership with Wandera, sold by IBM with the MaaS360 product. Although MaaS360's has many strengths, MaaS360 is missing some application management software packaging capabilities. However, support is given for importing packages created with other endpoint management solutions, such as a workflow to migrate applications from a Microsoft SCCM server into MaaS360. Strong patch management is given for iOS and Windows; however, patch capabilities for ChromeOS and Linux are unavailable. More recently, MaaS360 combined security settings that were once separated throughout the solution and consolidated them into a central policy to improve the visibility of all security settings with RBAC capabilities. These endpoint security policies, which are different from the management policies, include phishing, app permissions, privileges, and other device security settings. Also new is the solutions threat telemetry capabilities, such as device events, which MaaS360 currently supports a ZScaler integration. IBM Security MaaS360 with Watson gives remote support with TeamViewer supporting over-the-air (OTA) device views, remote configuration of devices, provision connectivity, and the ability to remediate issues.

MaaS360 can be offered as a standalone SaaS product to support enterprise organizations down to the SMB level. The product can support both public and government cloud environments. Cloud delivery gives full multi-tenancy. It can also be offered as a managed service, whether partially or fully managed by IBM services for full device lifecycle management or Device-As-A-Service. The product is implemented using a microservices

architecture supporting container-based platforms such as Docker and Red Hat. Almost all MaaS360 functionality is available via REST APIs and webhooks. Functionality via CLI is unavailable, but Android and iOS SDKs are available, focusing on DLP and Gateway capabilities. MaaS360 has been independently certified to comply with standards such as SOC 2, FedRAMP High Impact Level 2, ISA 27001, 27018, 27701, FISMA Moderate, and FIPS 140-2 cryptographic module standard.

The IBM MaaS360 continues to innovate and provide full spectrum UEM capabilities driven by AI capabilities supporting SMBs to large enterprises, making them a strong contender in the UEM market. IBM MaaS360 maintains a worldwide presence, although primarily in North America and the EMEA region, with significant growth in the Americas. IBM offers a large number of system integration partners on a global scale and substantial experience in large-scale deployments.

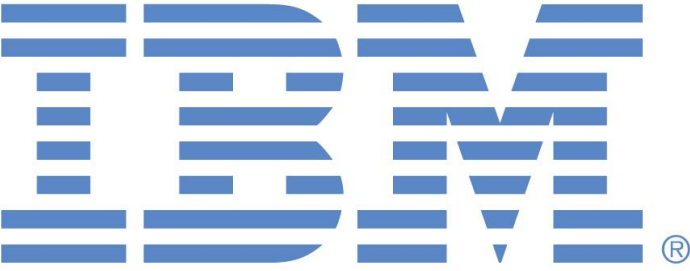
Security	Strong Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 7 IBM's rating

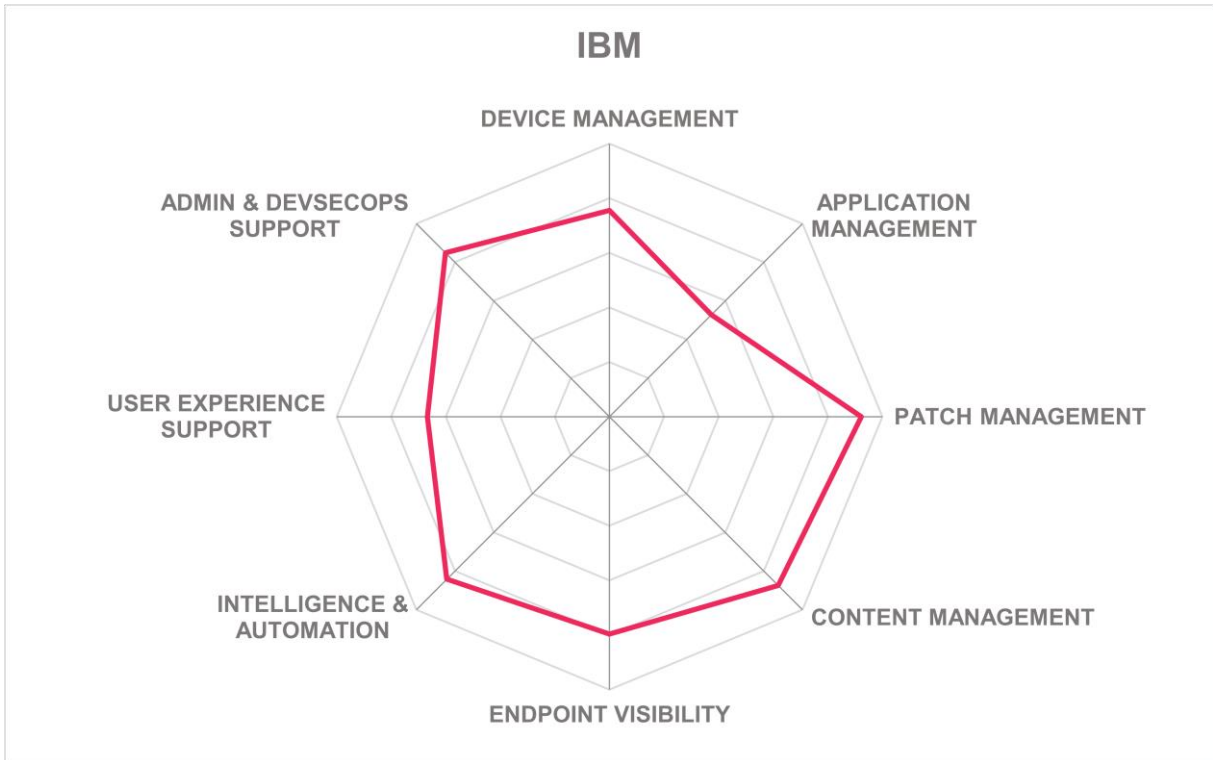
Strengths

- Strong patch management
- Good content management
- Strong endpoint intelligence
- Admin & DevSecOps support
- Device management
- User experience support
- Good range of supported endpoints
- Strong professional services and partner ecosystem

Challenges

- UEM primary focused in North America, followed by EMEA, with continued growth APAC and other regions.
- Primarily SaaS only without an on-premises IBM Cloud Extender
- Linux support is unavailable.
- Missing patch capabilities for Linux and ChromeOS
- Limited software packaging capabilities
- Requires integration with other IBM products for some more advanced features.

Leader in



Ivanti – Ivanti Neurons for UEM Premium with Security

Founded in 1985, Ivanti is a large, privately held company with 36 offices in 23 countries with headquarters in the Western US. Along with Ivanti's existing position as a global IT solutions provider, Ivanti has made a series of acquisitions starting in 2020, such as MobileIron, a mobile-centric UEM solution, Pulse Secure providing secure access and mobile security have strongly positioned Ivanti in the market UEM, as Ivanti Neurons for UEM solution. In 2021, Ivanti acquired Cherwell, a leading ITSM solution, and RiskSense, providing risk-based vulnerability management, further strengthening Ivanti's UEM market position when combined with RiskSense and Cherwell's offering. Ivanti's offering is a combination of Unified Endpoint Management, Cybersecurity, and Employee Experience Management (EXM).

Ivanti Neurons for UEM solution is a single platform with multiple products and services. The product provides a wide range of capabilities, including endpoint discovery, provisioning, configuration, real-time assistance, app management, monitoring, and security through patch management and other device and app controls, as well as threat defense. Except for endpoints such as business virtual assistants, or smartboards, Ivanti covers a wide range of endpoint types, and all endpoint operating systems evaluated are supported.

The UEM platform gives full endpoint lifecycle support with good third-party integration options. Patch management supports all operating systems evaluated apart from a Raspbian-based OS. Strong application software deployment and packaging features are given. Ivanti's discovery module finds software and hardware assets using active and passive scanners, then inventory them. Discovery module features in service mapping and SNMP extensions. Good endpoint content management is available. Ivanti gives solid endpoint security support with a wide range of out-of-the-box policies and templates provided for compliance. Ivanti Neurons for UEM solution's endpoint visibility includes a modern and helpful UI with detailed dashboards and access to a good set of out-of-the-box reporting options. Good user experience support is provided and enhanced by intelligence, such as detecting IT anomalies affecting users and DEX scoring. The use of Neurons bot automation allows for finding issues, with the ability to resolve the problems before they impact the user.

Ivanti UEM solution is implemented in a microservices architecture. It can be deployed as SaaS, software, or as an appliance (hardware or virtual) installed on a customer's premises or a public or private cloud service as well support for hybrid use cases. The cloud offering provides full multi-tenancy. A managed service is not offered, and container-based delivery is not available. Most of the solution's functionality is exposed by APIs, such as REST, SOAP, JSON-RPC, and XML-RPC, and most agent functionality on Windows systems can be initiated from CLI. SDKs are provided only for Android and iOS programming languages. Good authentication options are available for self-service access, although there is an extremely limited number of options given to administrators. The solution has been independently certified to support compliance with the FIPS 140-2, ISO/IEC 27001, ISO/IEC 15408, PCI-DSS v 3.2, US FedRAMP (moderate level), and CSPN standards.

Ivanti has a good market presence in North America and the EMEA regions, with growth in the APAC region. Ivanti's customer base comprises SMB to mid-market organizations with an increasing presence at the enterprise level. Ivanti continues to appear in all leadership

segments of this UEM Leadership Compass. Overall, Ivanti Neurons for UEM solution offers a well-balanced and flexible UEM offering with an innovative approach of converging UEM with user experience management and should be on the shortlist for organizations considering deploying UEM solutions.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive



Table 8: Ivanti's rating

Strengths

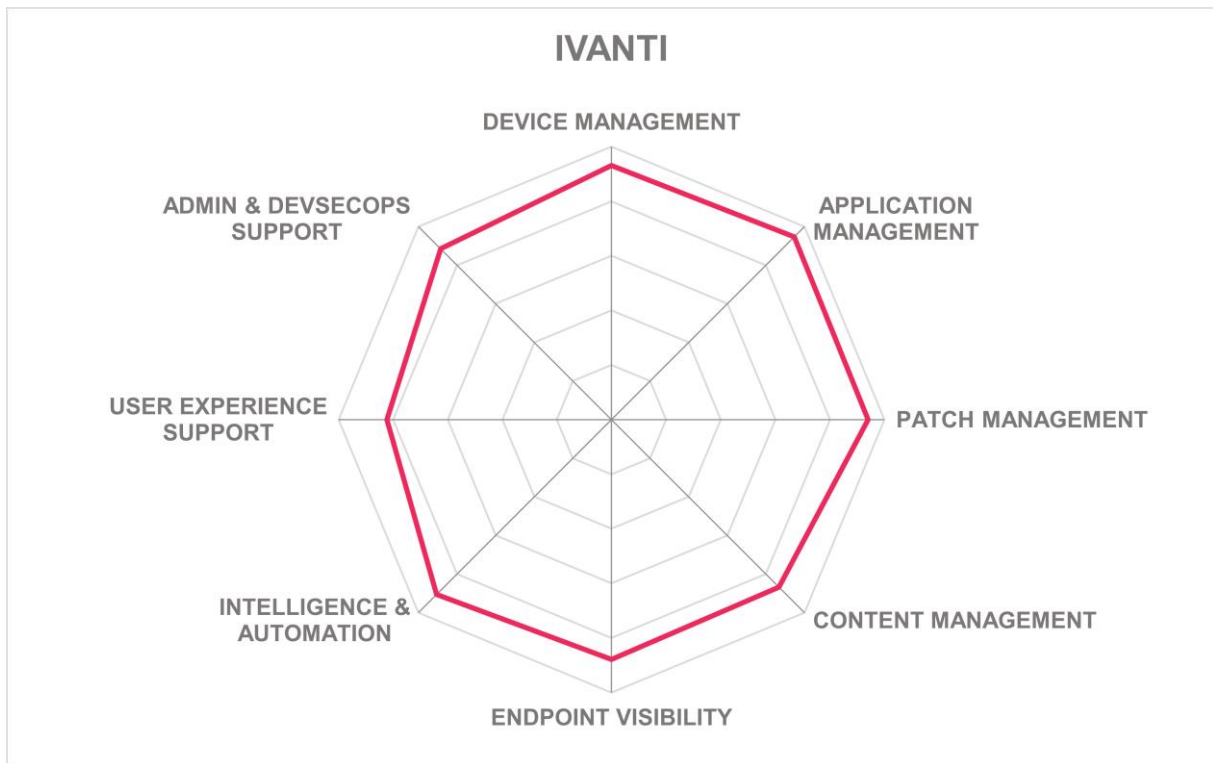
- Strong application management
- Strong application management
- Strong device management
- Strong patch management
- Good endpoint intelligence and automation
- Content management
- User experience support
- Admin & DevOps support
- Good partner ecosystem

Challenges

- A container-based delivery option is not available.
- A managed service is not offered.
- Limited SDK options.
- Experience management capabilities are built-in, and integrations with third party DEX or EUEM solutions are not available

Leader in





Jamf – Jamf Suite

Jamf has been a publicly traded company since 2020 and is headquartered in Minneapolis, MN. Jamf provides a single platform with a suite of products, a white-label solution, and managed service providers. In 2022 Jamf acquired ZecOps, extending their mobile security capabilities by adding advanced detection and incident response for iOS. The Jamf product offerings evaluated in this Leadership Compass include its Fundamentals Plan, Business Plan, Enterprise Plan, Jamf Pro, Jamf Protect (inclusive of Jamf Threat Defense and Jamf Data Policy), Jamf Connect (inclusive of Jamf Private Access), and Jamf School (inclusive of Jamf Safe Internet).

Jamf provides comprehensive endpoint device support from traditional desktops, laptops, and smartphones, to wearables, smartboards, IoT devices, mixed reality (VR) headsets, PoS Kiosks, ATMs, and server deployments, except for business virtual assistants (e.g., Alexa for Business). Supported endpoint operating systems include iOS, mac OS, Windows, a wide range of Linux distributions, and Chrome.

Jamf device onboarding allows for customization, automation, and integration with cloud identity providers. Workflows are available to enroll devices and deploy software. Jamf's application management includes an app catalog with over a thousand applications available and the Jamf patch definition feed. The solution also provides inventory management capabilities for hardware and software, security, device management, and operating system status. The patch management framework can update operating systems and applications. Out-of-date endpoint software and applications can be detected, including threats to the endpoints. Also available are on-device analysis and behavioral monitoring for threats and vulnerabilities, automated remediation controls, quarantine of malicious software, and data loss prevention through preventing access to unapproved storage devices. Jamf provides a modern web administration UI with useful dashboards and product navigation, with many OOTB reports available. The Jamf Threat Labs leverages threat researchers, cybersecurity experts, and data science primarily focused on Apple and mobile ecosystems, looking for vulnerabilities, threats, and data exposures, feeding back results into Jamf's security intelligence. Some user experience support is provided through basic health monitoring telemetry, detecting IT anomalies affecting users, and optimizing IT Service Management.

Jamf supports both on-premises and cloud deployment models and can deliver solutions as SaaS, virtual appliances, containers, software deployed to servers, or as a managed service. For cloud delivery, the product supports full multi-tenancy for all components. Jamf also maintains feature parity between Jamf's in-house and MSP services. The container-based delivery option supports Docker and Red Hat platforms. Almost all of Jamf's functionality is available via REST APIs and Webhooks. Jamf also provides access to capabilities via scripting and a wide range of SDK options. Support is given for compliance standards and guidelines such as SOC 2, ISO 27001, ISO 27701, Cyber Essentials, and CSA Start Level 1, with the US FedRAMP certification currently in process.

Jamf's customer base is SMB, Enterprise, Education, Healthcare and other industries with a good presence in the North American and EMEA region, an additional footprint in APAC and Latin America, and a particular focus on the education industry. Jamf provides a

comprehensive technology stack for the Apple platform that spans device management, user identity, application lifecycle, and security. For non-Apple devices, Jamf works closely with technology partners such as Microsoft and Google to provide device management functionality upon which the Jamf security technologies sit, ensuring that policy enforcement and end-user workflows remain consistent regardless of OS selected. Jamf’s core cloud platform technologies have evolved through acquisitions, and KuppingerCole expects Jamf to continue innovating in the UEM market. Jamf appears in all leadership categories in this Leadership Compass and should be on the shortlist when evaluating UEM solutions.

Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Strong Positive	

Table 9: Jamf’s rating

Strengths

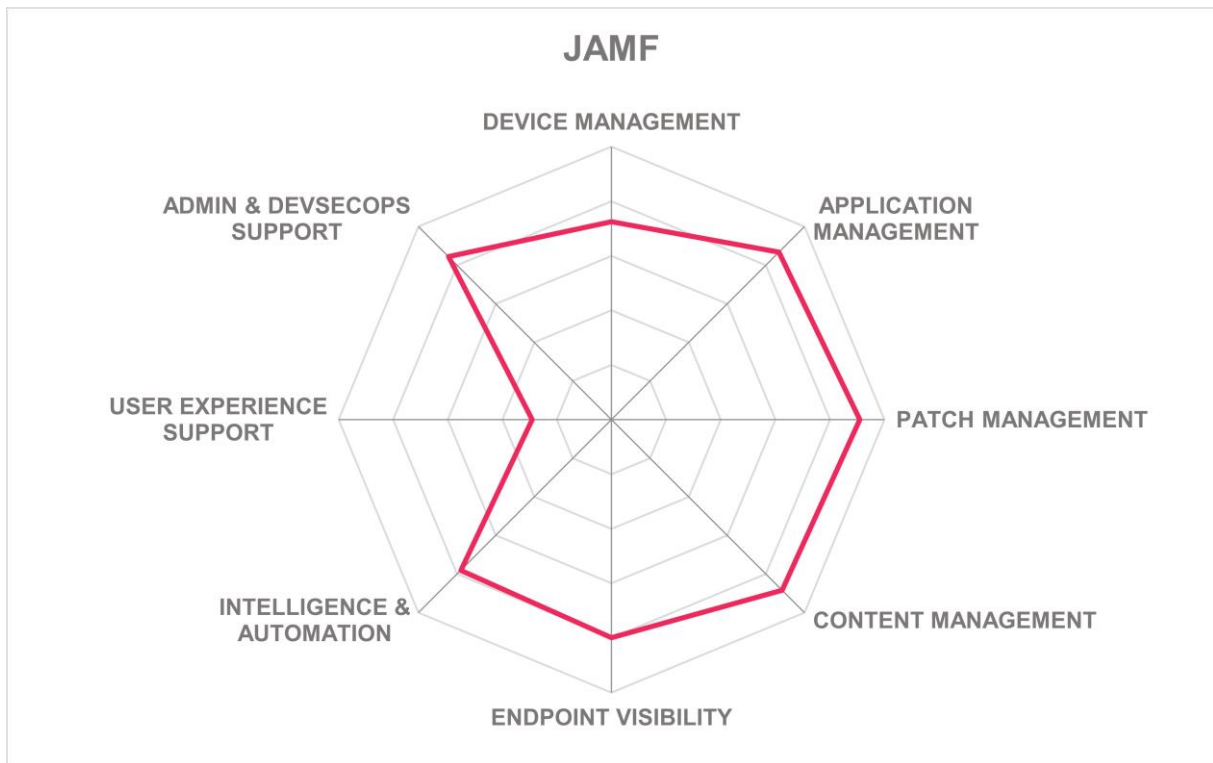
- Patch management
- Application management
- Content management
- Admin and DevSecOps support
- Endpoint visibility
- Intelligence and automation
- Device management
- Proactive threat detection and research through Jamf Threat Labs
- Good partner ecosystem
- Good third-party integration options

Challenges

- Third party dependencies to support Windows endpoints
- Container-based delivery offering are unavailable
- Little user experience support, although some DEX capabilities are on its near-term roadmap

Leader in





ManageEngine – ManageEngine Endpoint Central

Headquartered in Pleasanton, US, ManageEngine is under the umbrella of the India-based Zoho Corporation, founded in 1996. In 2002, ManageEngine was launched for Enterprise IT management, now offering ManageEngine Endpoint Central, formerly Desktop Central, a single set of products within its product portfolio as an integrated suite.

ManageEngine's Endpoint Central solution provides a single pane of glass for UEM capabilities, such as managing endpoint devices, applications, assets, expense, security, patch management, endpoint discovery, health monitoring, and endpoint intelligence, to name a few. ManageEngine supports a comprehensive set of endpoint types except for business virtual assistants. All endpoint operating systems evaluated are supported, including mobile iOS, Android, and Chrome, as well as good support for Windows, which includes Windows XP to Windows 11 version and devices running on Windows 10 IoT. Windows Phone 8.1 and above can also be managed through ManageEngine UEM. Also, support for macOS and Linux is given. ManageEngine also offers co-management options for legacy client machines.

Endpoint Central provides end-to-end device life-cycle management from device onboarding and application provisioning to device decommissioning and remote management. Also provided is the ability to automate app updates across major app stores. Device security includes web protection, data loss prevention, endpoint containment, conditional access, continuous vulnerability assessments and remediation, and anti-ransomware capabilities. Good workflow support is available such as enrollment of devices, automated provisioning of users, apps, content, and other resources, auto-remediation from device baseline security deviations, and managing updates by testing, approving, and scheduling updates. The solution provides patch management for Windows, macOS, Linux, and Chrome and update management support for Android custom firmware used in device types like rugged devices, scanners, etc. However, patch management for Raspberry Pi OS is not supported. Software package Creation and Distribution, OS imaging, and deployment are included, and pre-created software templates are given. ManageEngine provides many other auxiliary products and built-in capabilities such as ITSM, license management, asset management, etc., so there are limited integration options to other third-party solutions. However, integrations to Jira, Freshservice, ServiceNow, Spiceworks, and Zendesk are available. For Work-from-Anywhere use cases, ManageEngine is continuing to innovate through its Autonomous Digital Workplace by providing IT automation and end-user experience utilizing its endpoint security, management, and analytics capabilities.

Endpoint Central hosts on-premises, Zoho Cloud, and third-party and private clouds. ManageEngine has been independently certified as compliant with a wide range of standards and regulations, such as ISO, HIPPA, GDPR, CCPA, and TRUSTe, to mention a few. Although deployments to container-based platforms are unavailable, ManageEngine is delivered as SaaS, where Zoho is the cloud provider with data centers in North America, the EU, Asia, and Australia. ManageEngine also offers software for Managed Service providers to provide a managed service to the customer but does not manage the service themselves. Multi-tenancy is supported for their Remote Monitoring and Management (RMM). To access product functionality, only REST APIs are exposed. CLIs and SDKs are not available.

ManageEngine is well represented in the market with customers in North America and EMEA, followed by the APAC regions with growth in Latin America. Its customers are primarily in the Medium to Mid-Market, which extends into enterprise-level deployments. ManageEngine provides a good partner ecosystem as well as professional services. Overall, ManageEngine's Unified Endpoint Management solution offers a good balance of features and appears in all leadership segments in this UEM Leadership Compass.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive



Table 10: ManageEngine's rating

Strengths

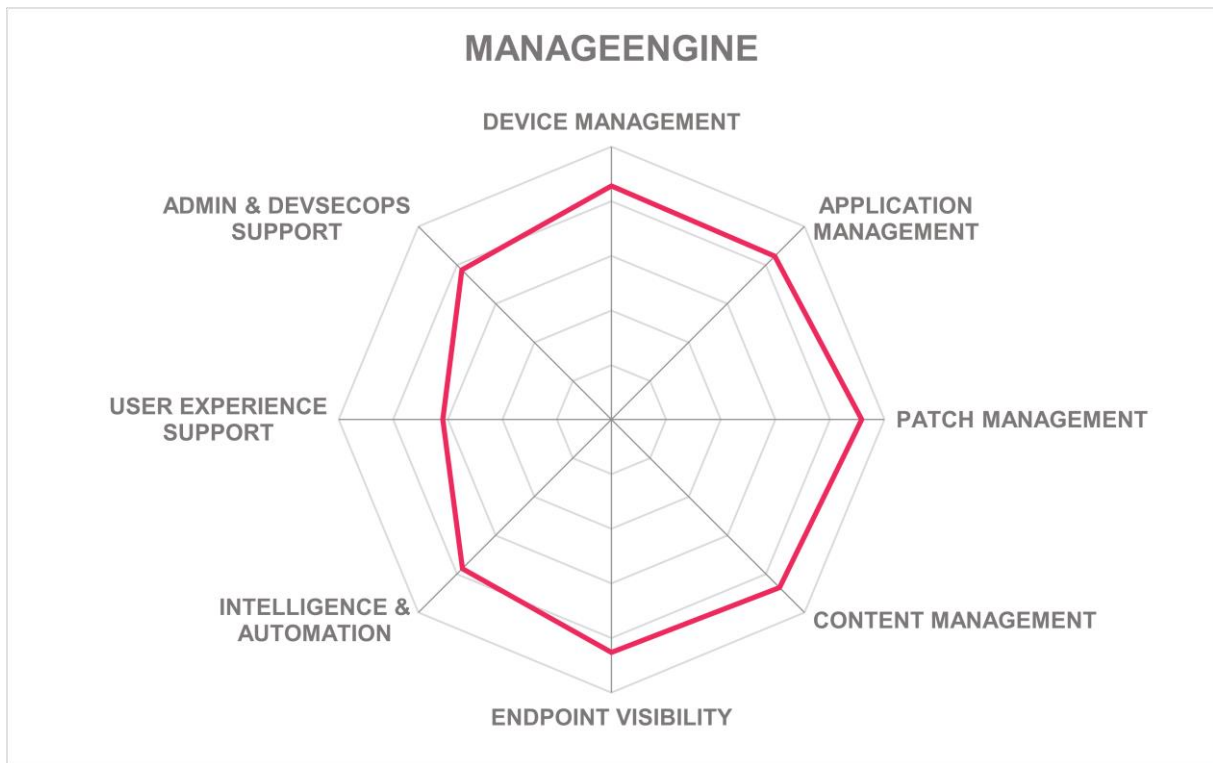
- Strong patch management
- Content management
- Device management
- Application management
- Endpoint visibility
- Intelligence and automation
- Admin & DevSecOps support
- User experience support
- A well laid out and user-friendly web UI.
- Good partner ecosystem and professional services

Challenges

- Missing CLI and SDK support
- Only RESTful APIs provided, no other options.
- Limited third-party integration options
- Limited authentication options for self-service and administration access
- Deployments to container-based platforms (e.g., Docker, Red Hat) are unavailable

Leader in





Microsoft – Microsoft Intune

Microsoft Corporation is one of the largest technology companies worldwide, headquartered in Redmond, Washington. Microsoft's UEM solution has shifted its focus to its cloud solution, Intune. As such, Microsoft has recently renamed Microsoft Endpoint Manager back to Microsoft Intune. Microsoft Configuration Manager is still a component of the Intune family. Microsoft's Intune solution provides core UEM capabilities such as device enrollment, application management, policy enforcement, and conditional access while keeping endpoints updated and compliant. Microsoft Intune Suite includes Intune Remote Help, Intune Endpoint Privilege Management, Microsoft Tunnel for Mobile App Management, advanced app management, and advanced endpoint analytics features on the near-term roadmap.

Along with Microsoft Intune's product focus of core UEM and Intune Suite of products, extensions can be made through Microsoft Defender for capabilities such as endpoint discovery, Mobile Threat Defense (MTD), and Digital Employee Experience (DEX). However, some abilities, such as Mobile Identity Management (MIM) functions, depends on Azure Active Directory P1, and Mobile Content Management (MCM) requires OneDrive. All areas of endpoint device support are covered, including desktop, mobile, tablets, wearables (e.g., smartwatches), and IoT, with additional device support via ConfigMgr for servers. Except for Chrome OS, most endpoint operating system support is given, including iOS, Android, and Windows, and increased support for macOS and Linux. Support for business virtual assistants, smartboards, and TV OSs is unavailable.

Some of the UEM solution's newest features are offered within the Intune Suite. Intune Remote Help provides remote assistance connections to endpoint devices with role-based permissions, which are auditable. For example, it checks for device compliance before the remote session starts, and it can also provide root cause visibility for non-compliant devices. Intune Endpoint Privilege Management allows for the definition of elevated permissions to administrators for specific tasks and will be offered as a stand-alone add-on for Windows at first. Microsoft Tunnel for Mobile Application Management gives Android and iOS mobile devices a microVPN in BYOD scenarios, for example, where admins don't want employees to enroll their devices but use Microsoft's MAM-only mode instead. Its automated app patching capabilities help mitigate vulnerabilities and simplify packaging and deploying applications to Windows and Mac endpoints. Advanced Endpoint Analytics can detect and report tenant and device anomalies with near real-time correlation to events and use signal and scope tags when reporting on devices.

Since Intune inherits the capabilities of Configuration Manager, both on-premises and cloud deployment models are supported, with the cloud service delivered as SaaS running on the PaaS on Azure. Also, components of Configuration Manager can be deployed as Azure roles or IaaS. A hybrid deployment model can be accomplished by using Configuration Manager for on-premises and Intune in the cloud. Intune is offered as a managed service through Microsoft Managed Device. Intune capabilities are accessible via its Microsoft Graph (REST) API only, although some private APIs for specific security-related items, such as compliance data, are also offered. CLI support is given via PowerShell, which can access the entire Graph API. SDKs are available for Android, iOS, Java, C/C++, .NET, and Swift. Microsoft

Intune has been independently certified to comply with a comprehensive set of standards such as FIPS 197 and FIPS 140-2, NIST 800-57, PCI-DSS v 3.2, HIPAA/HITRUST, and US FedRAMP.

Since its founding in 1975, the Microsoft Corporation has grown to have one of the largest market presences in just about every part of the world with strong support, professional services, and a partner ecosystem. Microsoft has the infrastructure and capability to scale extremely high workloads and is continually expanding support to other device platforms beyond its own. Microsoft continues to be one of the leaders in the UEM space, as indicated by appearing in this Leadership Compass report's Product, Market, Innovation, and Overall, Leader segments. Microsoft Intune should be on the shortlist for organizations considering deploying UEM solutions.

Security	Strong Positive	 Microsoft
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 11: Microsoft's rating

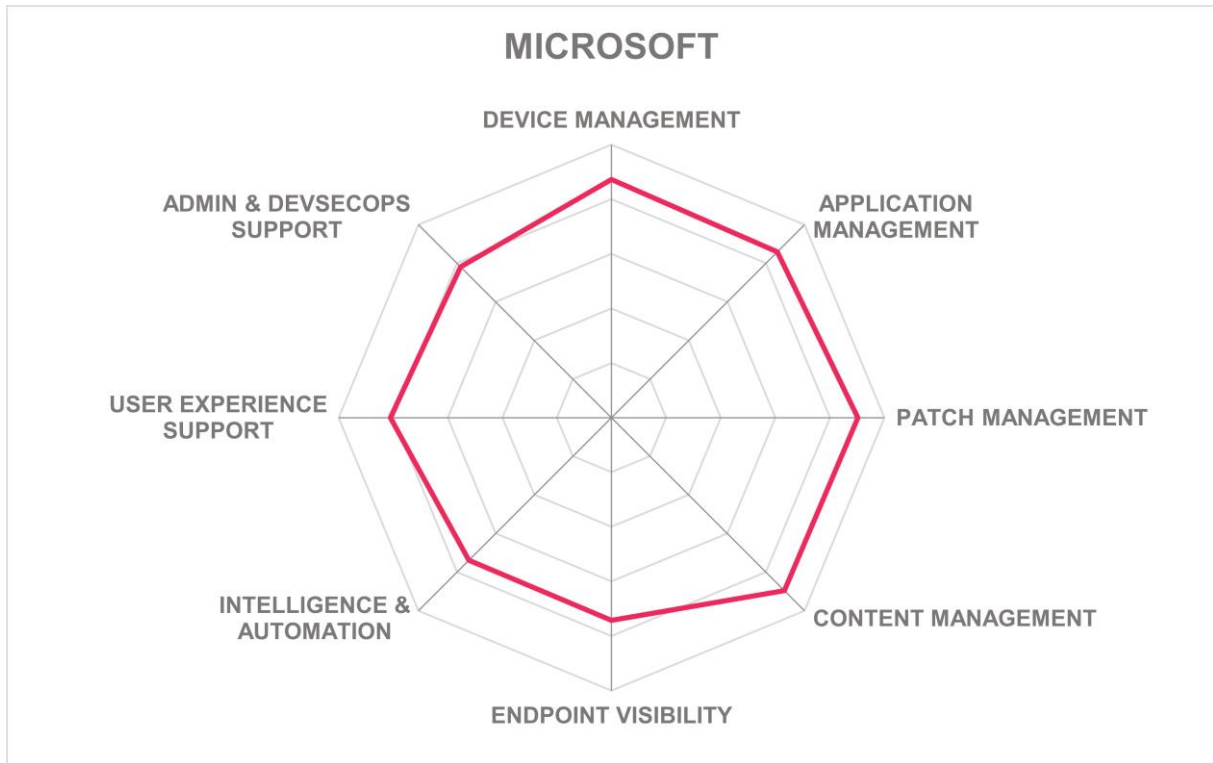
Strengths

- Strong Patch management
- Strong Device management
- Good Content management
- Good Application management
- User experience support
- Admin & DevSecOps support
- Endpoint intelligence and automation
- Wide range of endpoint type support
- Good, unified admin UI console
- Strong support and partner ecosystem

Challenges

- Dependences on other Microsoft services such as Azure Active Directory
- Limited pre-defined compliance reports out-of-the-box
- Private cloud deployment option is not available

Leader in



Miradore – Miradore

Founded in 2006, Miradore is a privately held company based in Finland. The product, also called Miradore, is a cloud-based Mobile Device Management platform reviewed in this Leadership Compass.

Miradore offers device, application, asset, and patch management with software package creation and distribution capabilities. Device provisioning, health monitoring, and tracking are also included. Some endpoint intelligence and endpoint discovery features are given, and remote access management for remote troubleshooting and integration to TeamViewer remote control. Support is given to traditional endpoint device types such as desktops, laptops, tablets, and smartphones. Point-of-sale kiosks and industrial mobile devices use cases support is also available. Miradore can manage endpoint operating systems such as iOS, Android, Windows, and macOS, although Linux and Chrome are unavailable.

Endpoint lifecycle management includes automated onboarding of users and provisioning of applications. The solution also provides automatic enrollment and remote troubleshooting and locking and/or wiping of endpoints. Miradore also offers endpoint discovery capabilities and keeps a repository of discovered endpoint hardware and software information. Workflows are provided for acquiring device activity status, purchase, and lease information. Also, an analysis of discovered endpoints can be conducted, and checks for vulnerabilities and compliance (e.g., missing patches). Endpoint patch management is limited to iOS and Windows, which is well supported through patch updates, rollout options, automatic approvals with Windows patching, testing, piloting, and approval of patches before release. Miradore's patch feed provides Windows updates and patches for hundreds of software products from almost 100 software vendors, in which the feed is continuously updated with new patches, products, and vendors. Application software deployment and packaging allow for application whitelisting or blacklisting for iOS and Android. The solution provides a graphical packaging UI for creation and customization. Miradore business policy can contain a set of applications, files, certificates, and configurations. If missing, they can be automatically deployed.

Miradore provides a single platform. The solution is available as a SaaS on the public cloud or through managed service providers. Some of Miradore's functionality is accessible via REST APIs, although access through CLI or SDKs is not provided. Custom integration with third-party services like ITSM, threat intelligence, EEP, or EDR can be accomplished via API. The Miradore UI has an easily understood layout with color risk indicators, a helpful dashboard that includes many OOB widgets, and an MSP portal for partners managing customers. The Miradore solution is in the process of being independently audited to comply with ISO/IEC 27001.

Miradore supports SMB to mid-market customers concentrated in the EMEA and North America region, although showing growth in APAC, Latin America. SMBs and MSPs requiring basic endpoint device and application capabilities with good patch management can consider Miradore for evaluation.

Security	Neutral	
Functionality	Weak	
Deployment	Neutral	
Interoperability	Neutral	
Usability	Neutral	

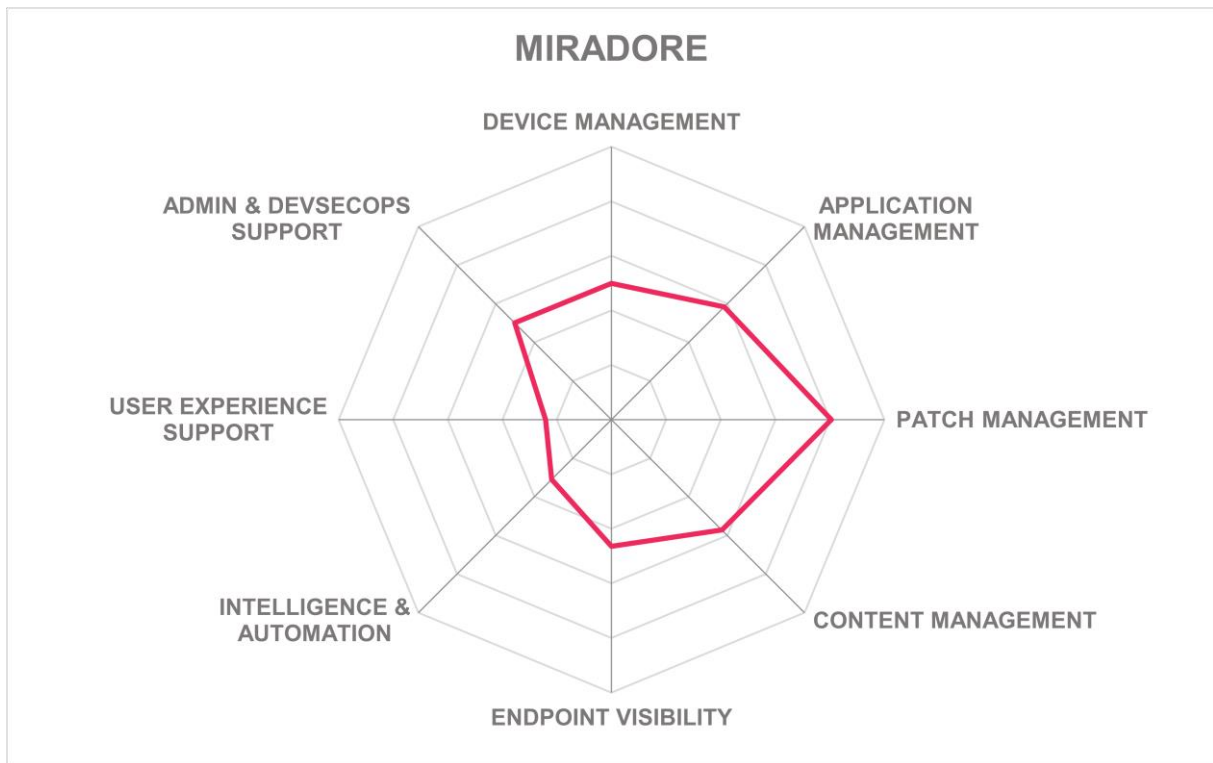
Table 12: Miradore's rating

Strengths

- Patch management
- Application management
- Content management
- Asset management
- Well laid out and useful UI
- MSP portal for partners managing customers

Challenges

- Small partner ecosystem
- Limited support services
- Limited device management
- Admin & DevSecOps support
- Weak user experience support
- Weak endpoint intelligence
- Missing support for both Linux and Chrome OS



OpenText (Micro Focus) – ZENworks Suite

Micro Focus is a global infrastructure software business that was founded in 1976 and headquartered in Newbury, UK. In January 2023, OpenText™ announced that it had completed its acquisition of Micro Focus through its wholly owned subsidiary, OpenText UK Holding Limited. The OpenText-Micro Focus offers a suite of products for Unified Endpoint Management, which includes features from ZENworks Configuration Management, ZENworks Patch Management, ZENworks Full Disk Encryption, ZENworks Endpoint Security, ZENworks Asset Management, ZENworks Service Desk, and Hybrid Workspaces.

The OpenText-Micro Focus UEM solution offers endpoint device, application, content, patch, license, asset, and mobile identity management, as well as endpoint discovery tracking and security as examples of the suite's capabilities. However, endpoint device health monitoring is not given. Micro Focus features include policy-driven endpoint backup and recovery for Windows and macOS devices with in-built file sync and share capabilities via its Connect MX solution. Also noted is that Mobile Content Management is provided via Filr, Voltage SmartCipher, and Mobile Device Archiving & eDiscovery is provided via Retain Information Archiving. Apart from more advanced device types, such as wearables (e.g., Apple Watch), IoT, printers, virtual business assistants, or mixed reality headsets, Micro Focus gives good support to traditional types of endpoint devices such as desktops, laptops, smartphones, and tablets, with the additional support for smartboards, and TV OS, ATMs, Point of Sale Kiosks and industrial mobile devices. Most operating systems are supported, except for Chrome.

Micro Focus ZENworks endpoint lifecycle management supports endpoint provisioning of devices and applications. The lifecycle management provides a hardware and software inventory, distribution, configuration, patch management, remote support, backups, and license tracking. For endpoint device end-of-life, device wiping is available. The solution also provides endpoint application containerization and application streaming capabilities. As part of its endpoint security management offering, integrated anti-virus/anti-malware capabilities are available. Hybrid Workspaces is a white-labeled product featuring ZENworks integration. In addition to ZENworks Service Desk, the solution can integrate with third-party ITAM and ITSM. This ITSM tool integrates easily with ZENworks to assist in remote management, software deployment, configuration management, and requesting services through the ITSM portal. Other OOB third-party endpoint solutions integrations are limited. The solutions endpoint provisioning covers users, devices, and applications. It is possible to package applications using either the AdminStudio Standard Edition tool or Hybrid Workspace packaging that can containerize an application to stream or run on a device in its workspace. ZENworks rule-based patch policies allow automated and scheduled installation of patches. Patch compliance dashboards in the management console automate information collection and display the patch status of devices. It also integrates with the NIST CVE database providing a CVE-based view of the environment.

OpenText-Micro Focus ZENworks provides a modern, detailed, and complex centralized UI with a good set of out-of-the-box reports and user self-service. Dashboards allow drill-down details with customizable dashlets. Micro Focus ZENworks is also moving towards a microservice-based architecture direction over time. It offers a traditional installer that runs on Windows or Linux that can be deployed on-premises or on a cloud-hosted VM. Linux

installments require Docker and a file-based microservice on Windows installments. Also offered is a pre-built virtual appliance that includes Docker and is available for Hyper-V, VMware, and Citrix virtualization platforms. For Cloud, the solution supports Windows or Linux server cloud deployments. Currently, the cloud offering does not support multi-tenancy. Also, ZENworks provides an administrative SOAP interface, and a limited amount of functionality is available via REST, which includes its reporting engine. Some CLI access to functionality is provided, although SDK support is not.

OpenText-Micro Focus has a good global presence and partner ecosystem. The ZENworks suite and Hybrid Workspaces offer a set of UEM capabilities with strength in patch, device, and application management. With Micro Focus's recent acquisition by OpenText, it will be interesting to see how it will grow its UEM feature set. The OpenText-Micro Focus UEM solution could be particularly interesting to existing Micro Focus customers who can take advantage of the other OpenText-Micro Focus product integrations.

Security	Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Neutral	
Usability	Positive	

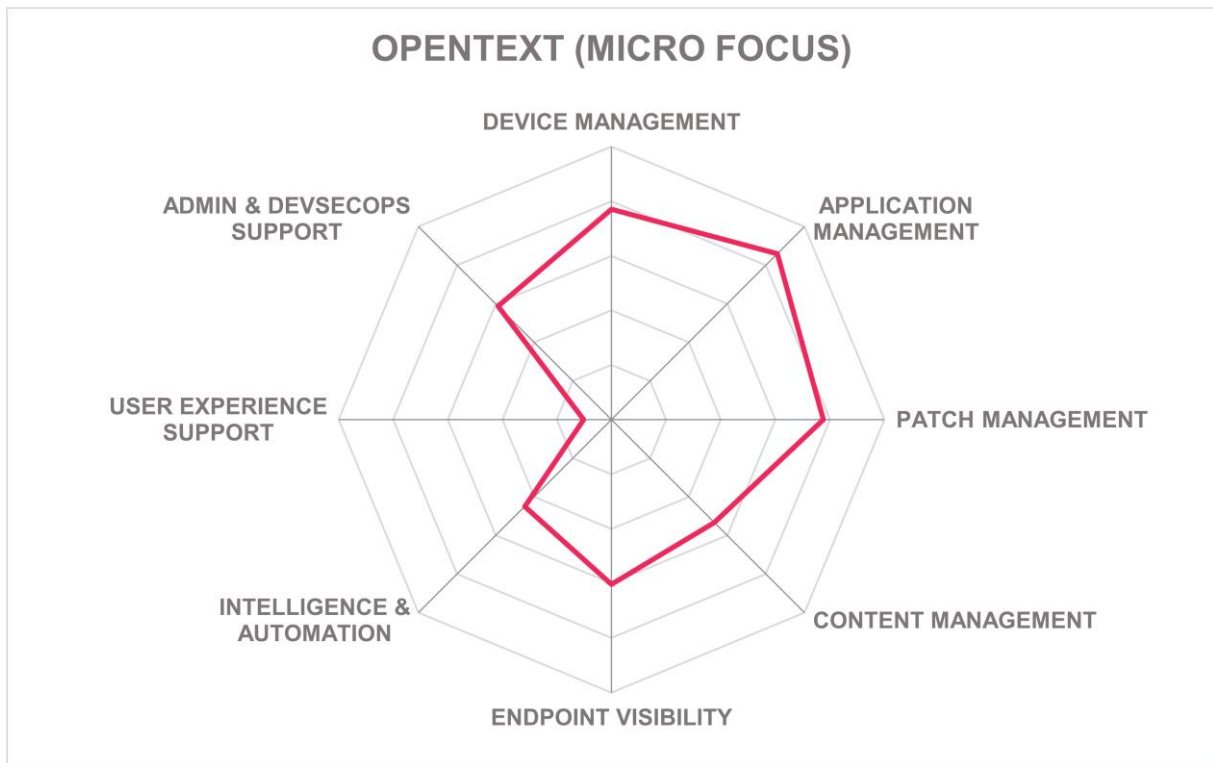
Table 13: Micro Focus's rating

Strengths

- Good Application management
- Patch management
- Device management
- Endpoint visibility
- Good OOB reporting
- Enterprise-level family of product offerings
- Support and professional services

Challenges

- Product offering components are sometimes complex to understand and implement
- Limited endpoint intelligence
- Some API limitation
- SDK support is missing
- Missing Chrome OS support
- Very limited user experience support



KACE by Quest

Quest is a privately held software company headquartered in Aliso Viejo, California. Although Quest was founded in 1987, KACE by Quest Unified Endpoint Management was founded in 2003. The KACE by Quest UEM solution, considered in this Leadership Compass, is comprised of the KACE Unified Endpoint Manager (UEM) for a hybrid environment, KACE Cloud, and KACE-as-a-Service (KaaS) from the KACE suite of products. KACE Cloud offers cloud-based patch management, deployment of devices, remote lock, wipe, change passwords, or reset of devices, and automated policy management, while KaaS allows for cloud management of endpoints.

The KACE by Quest UEM solution centers on capabilities such as endpoint device, application, patch, license, content, asset management, endpoint security, device provisioning, endpoint discovery, health monitoring, and location tracking. Other capabilities, such as endpoint identity, expense management, or mobile threat defense, are not supported. Except for wearable consumer devices, virtual business assistants, and mixed reality headsets, all other device types are supported, including desktop, mobile, tablets, IoT, printers, smartboards, point-of-sale kiosks, ATM, and other industrial use cases. KACE by Quest supports a wide range of endpoint operating systems: iOS, Android, Windows, macOS, Linux, and ChromeOS.

Endpoint life cycle management includes endpoint provisioning of users, devices, applications, and content, and a built-in service desk can accomplish automated onboarding via ticket processes. KACE by Quest offers ITSM and ITAM capabilities out of the box. Endpoint activation and decommissioning are available. Remote access to endpoint devices requires a third-party integration, although the solution provides remote locking and wiping of endpoints for iOS, Android, Windows, and macOS. OS image creation is not part of the KACE by Quest UEM solution, but KACE by Quest does offer a system deployment solution for image creation, deployment, and management. The KACE by Quest patch management features are strong, giving good support to iOS, Android, Windows, macOS, and even Raspbian-based firmware. The solution provides the ability to scan & detect endpoint software version, patch level, and health. KACE by Quest's built-in reporting engine and dashboards leverage analytic data. Additional insights can be gathered via integrations leveraging KACE by Quest APIs or direct read-only database access. Both user self-service and admin access to its portals are supported through some good authentication options and MFA.

On-premises, cloud, and hybrid deployment scenarios are supported with SaaS, virtual appliances, software deployed to a server, serverless platforms, and managed service deployment models available. KaaS is delivered as SaaS. Container-based platforms are not supported. Only REST APIs are available for access to KACE by Quest functionality. Both CLI and SDK access to product features is available.

KACE by Quest customer base is concentrated in North America with a growing presence in the EMEA and APAC regions and is focused on SMB to mid-market organizations but can scale to the enterprise and provides good support and professional services. Quest continues to improve its UEM product portfolio and has become a Leader Overall, and in the

Product and Market segments. Overall, KACE by Quest is worthy of consideration, particularly for customers in North America with requirements focused on the endpoint device, application, and patch management.


Security	Positive	
Functionality	Positive	
Deployment	Positive	
Interoperability	Positive	
Usability	Positive	

Table 14: KACE's rating

Strengths

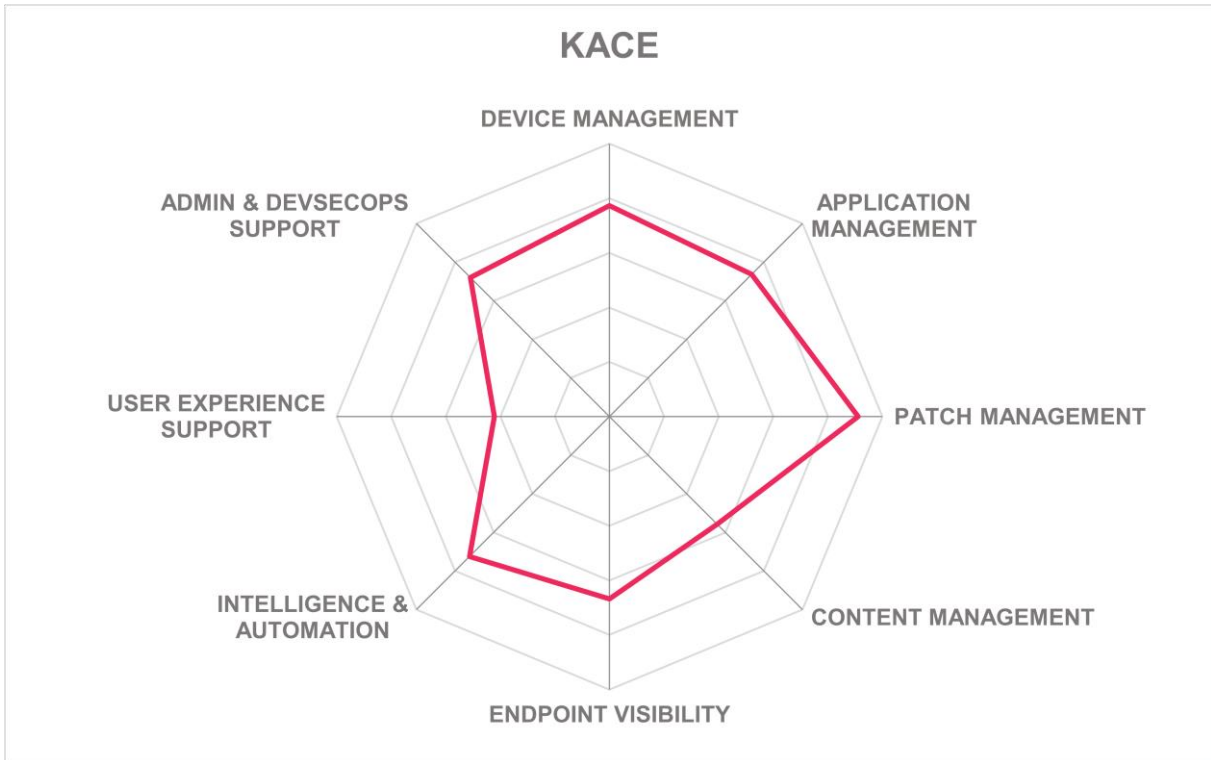
- Good patch management
- Device management
- Application management
- Product intelligence and automation features
- Endpoint visibility
- Some good user self-service and admin authentication options
- Inventory & Asset management
- Wide range of endpoint OS support
- Good support & professional services

Challenges

- Primarily concentrated in the North American market, while some presence in EMEA, LatAm & APAC regions
- Focused on SMB to mid-market organizations, although scalable to enterprise
- Limited content management
- Limited user experience support
- CLI and SDK support is not given
- OS image creation, deployment, and management requires an additional KACE solution, System Deployment Appliance (SDA)

Leader in





Sophos – Sophos Central

Sophos is owned by the private equity firm Thoma Bravo and is headquartered in Santa Clara, CA. Sophos provides a single platform that supports multiple products for endpoint, network, and email security, with underlining threat intelligence. Tangential to Sophos endpoint security is its cloud workload protection offering for securing a customer's cloud environments and resources within them, such as the AWS, Azure, and GCP environments, and it can monitor misconfigurations to increase usage costs. Underneath the Sophos central platform ecosystem is a data lake of customer data ingested from each Sophos product, allowing the customer to monitor and apply analytics and AI against different events across their suite of products. Sophos Central is its UEM solution that is evaluated in this Leadership Compass.

Sophos's UEM offering includes endpoint identity, device, and application management, with patch and expense management. Endpoint devices can be provisioned, tracked, and monitoring of the device's health. Endpoint discovery, intelligence, threat defense, privileged management, remote access, and troubleshooting. Supported endpoint types include traditional desktops, laptops, tablets, and smartphones. Point of Sale kiosks, ATMs, and industrial mobile devices are also supported. Other endpoint devices such as wearables, IoT, printers, smartboards, and mixed reality (VR) headsets are not. Sophos supports a good range of endpoint operating systems like Windows, iOS, macOS, Linux, Android, and Chrome.

Sophos Central provides core endpoint lifecycle management capabilities from provisioning of end-user devices, which is possible based on group and role assignments, to decommissioning endpoint, including the ability to wipe a device remotely. Although support for creating, deploying, and managing OS images is not given, there is good visibility of endpoint device information, the ability to synchronize endpoint users with Microsoft Active Directory, and remote endpoint device access support. One of Sophos Central's strengths is its extended detection and response (XDR) capabilities, which provide visibility through a SQL query framework, allowing queries to support threat investigation using endpoint telemetry from the Sophos data lake. Patch management is limited to iOS and Android devices. Endpoint containment and content management are accomplished through the Android Work Profile and Apple User enrollment management secure data and segregating corporate data from personal data. Sophos provides a centralized single pane of glass for its endpoint management. Sophos includes many reports out-of-the-box, such as device monitoring, tracking, and provisioning, as well as endpoint discovery results and mobile threat response. Sophos Live Response feature provides endpoint remediation through its remote support, as well as integration with TeamViewer for mobile devices.

Sophos Central is implemented in a microservices architecture, deployed to the public cloud, and delivered as SaaS. Other delivery options are not supported, such as container-based, hardware, or virtual appliances. Sophos also offers a fully managed detection and response security solution, which can leverage information from multiple Sophos and third-party products, including Sophos UEM. Only a small portion of the Sophos solutions capabilities are available through REST APIs. CLIs and SDKs are not available. Integrating third-party solutions such as ITAM, ITSM, and DEX/EUEM is possible using Sophos Central APIs.

Sophos has increased its endpoint intelligence capabilities through existing and acquired cybersecurity company technology and provides core mobile device UEM capabilities with strength in detection and response capabilities. Sophos's customer focus is SMB organizations with some presence in mid-market and enterprise companies located primarily in the North American and EMEA regions. Professional services are offered in each major region of the world.

Security	Positive	
Functionality	Neutral	
Deployment	Neutral	
Interoperability	Positive	
Usability	Positive	

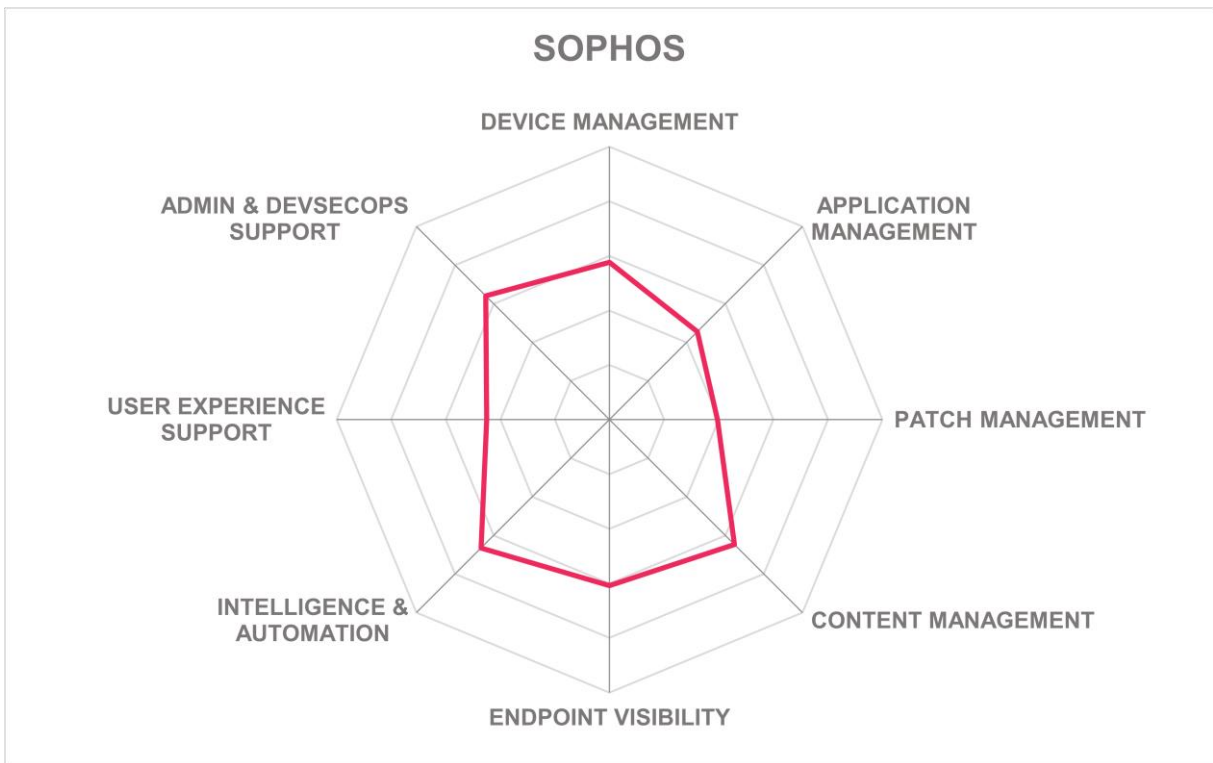
Table 15: Sophos's rating

Strengths

- Content management
- Endpoint visibility
- Good endpoint management intelligence and automation
- Threat defense capabilities
- Some user experience support
- Admin and DevSecOps support

Challenges

- Narrow focus on supported types of endpoint devices
- Weak application management capabilities
- Limited patch management
- Limited access to product capabilities via API and limited API options
- Missing CLI and SDK support
- Limited set of user self-service and admin authentication options



VMware – VMware Workspace ONE

VMware is a US company listed on the NYSE. VMware provides large-scale enterprise virtualization and cloud infrastructure solutions. More recently, Broadcom announced its intent to acquire VMware - to be completed within Broadcom's fiscal year, which ends after October 2023. Workspace ONE Unified Endpoint Management (UEM) is part of VMware's growing portfolio. Its Unified Endpoint Management is a component of its VMware Anywhere Workspace Platform that also integrates virtual apps and desktops, endpoint security, remote support, advanced analytics, and Digital Employee Experience (DEX). The platform shares unified administration, analytics, automation, workflow, and identity capabilities. VMware Workspace ONE, as a single platform with multiple services, is evaluated in this Leadership Compass.

Workspace ONE UEM is offered as a cloud-native client management solution intending to work on any endpoint, on any platform, with intelligence-driven automation capabilities. It provides a wide range of capabilities, including endpoint device, identity, content, patch, asset, and license management. Also offered are device provisioning, health monitoring, and tracking capabilities. Interestingly, it does not offer Endpoint Discovery capabilities, which would enhance its already feature-rich offering. Almost all areas of endpoint device support are covered, including desktops, laptops, tablets, smartphones, wearables, and printers, with additional device support for business virtual assistants, TV OS, mixed reality headsets, and point-of-sale kiosks, as well as rugged devices, Infinite Peripherals Sleds, and OS-less devices like beacons, IoT devices with x86_64 or ARM architecture. However, smartboards, ATMs, SNMP devices, or server endpoint types are not supported. All endpoint operating systems evaluated, such as iOS, Android, Windows, macOS, Linux, and Chrome, are supported. Additionally, Tizen's support is given, as well as IoT, shown through its support for Win10 IoT and Raspberry Pi.

Complete endpoint lifecycle management is provided, such as device provisioning, activation, and decommissioning. Workspace ONE also supports out-of-the-box (OOB) enrollment options for Android, iOS, macOS, Chrome OS, and Windows endpoints. Patch management includes iOS, Android, Windows, macOS, Linux, and Chrome support. Patch automation is based on CVE vulnerabilities and includes intelligent real-time patch compliance tracking. Workspace ONE provides a built-in automation and orchestration engine to orchestrate workflows and automated actions based on predefined policies. Workspace ONE Freestyle Orchestrator allows for low-code configuration workflow orchestration, such as with onboarding scenarios, using a drag-and-drop graphical UI editor. Also given are risk analytics and intelligence by leveraging ML models that monitor user behavior and calculate user risk scores. Its Digital Employee Experience Management (DEEM) provides ML-based insights to calculate a baseline for each parameter in the user environment. It proactively alerts administrators when anomalies and values fall outside a normal range, such as a higher-than-normal app crash rate. Strong authentication options are given for user self-service and admin access to the Workspace ONE UEM portals. The Workspace ONE UEM UI is modern and straightforward, with many useful graphics and dashboards. Good options for third-party integration are available such as an OOB integration with ServiceNow for ITSM. Other integrations, such as third-party threat intelligence and EDR, are supported via Workspace ONE Trust Network.

VMware Workspace ONE UEM can be deployed as software installed on a customer’s premises as well as public, private, or government cloud services, hybrid, or managed services. A Docker container-based delivery is also supported. For on-premises deployments, the Workspace ONE UEM Cloud Connector (a.k.a. AirWatch Cloud Connector) and the Unified Access Gateway server components are required, as well as a Microsoft SQL Server database. Cloud solutions are multi-tenant. Less than half of Workspace ONE UEM functionality is accessible via APIs, which includes SOAP and REST. However, both CLI access and SDKs for Android, iOS, Java, C/C++, Cordova, and Xamarin are supported. The product has been independently certified to support compliance with many standards such as FIPS 140-2, NIST 800-57, PCI-DSS v3.2, HIPAA/HITRUST, US FedRAMP moderate, DISA IL 2, ISO 27001, 27017, 27018, SOC 2 Type2, Cyber Essentials Plus (UK), and Cloud Security Alliance STAR Level 1 to name a few.

VMware supports a large customer base worldwide with its products and professional services. Overall, Workspace ONE UEM offers a well-balanced set of UEM capabilities with strong support for many security standards. VMware support for Work-from-Anywhere scenarios shows innovation that moves its product in a positive direction. VMware appears in all leadership categories of this Leadership Compass and should be on the shortlist for organizations considering UEM solutions.

Security	Strong Positive	
Functionality	Strong Positive	
Deployment	Strong Positive	
Interoperability	Strong Positive	
Usability	Strong Positive	

Table 16: VMware’s rating

Strengths

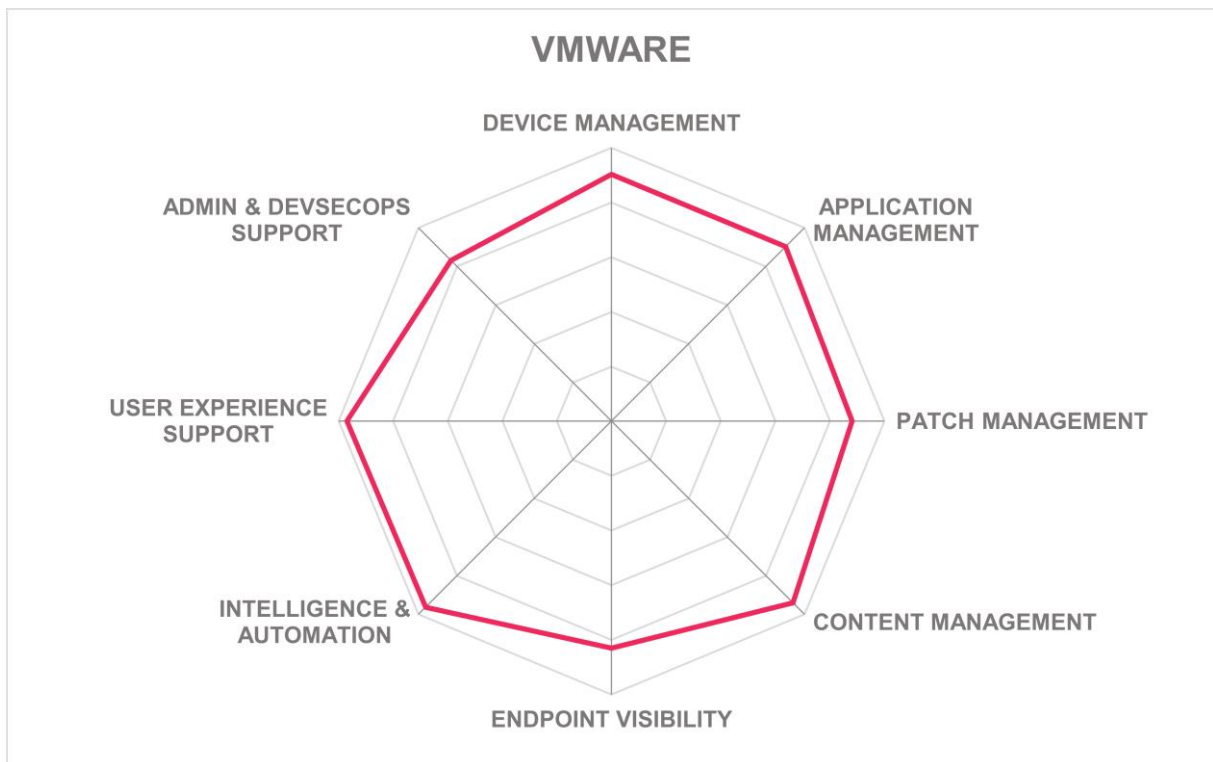
- Excellent user experience support
- Strong intelligence and automation capabilities
- Good device management
- Good Content management
- Patch management
- Application management
- Admin & DevSecOps support
- Good integration options
- Positive partner ecosystem

Challenges

- Limited functionality accessible via APIs
- Only Docker is supported as a container-based delivery option

- Microsoft SQL Server database is required for on-prem deployment
- The effects of the recent acquisition by Broadcom could leave the product strategy uncertain.

Leader in



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other vendors in the market that readers should be aware of. These vendors do not fully fit the market definition but offer a significant contribution to the market space. This may be for their supportive capabilities to the solutions reviewed in this document, for their unique methods of addressing the challenges of this segment or may be a fast-growing startup that may be a strong competitor in the future.

42Gears

Founded in 2009, 42Gears is a medium-sized private enterprise headquartered in Bangalore, India, of the APAC region, and an office in Fremont, CA. Under their portfolio of products, 42Gears offers Unified Endpoint Management tools to manage various types of endpoints and their apps and content.

42Gears SureMDM provides lifecycle management for endpoint devices such as Android, iOS, Linux, macOS, Windows, Google Wear OS, and Virtual Reality (VR) headsets. Other endpoint device solutions include SureLock for locking down devices used as a self-service Kiosk and SureFox for securing device browsers. In addition, CamLock gives the ability to secure device cameras to protect sensitive data in the workplace.

Why worth watching: 42Gears provides a unified set of solutions such as MDM lifecycle support, including device enrollment, application and content management, location tracking, and support for Kiosk use cases.

AppTec360

AppTec360 is a privately owned company with headquarters in Basel, Switzerland. Its Enterprise Mobility Management solution supports device management of its lifecycle, policies, applications, security, and content. Also supported are device service and expense management. Supported operating systems include Android, iOS, macOS, and Windows.

The AppTec360 system architecture consists of the EMM server managed through the AppTec360 EMM console and device access through its Universal Gateway. The solution's web console gives a unified view of its management capabilities, including device inventory, device details, and dashboard graphics and reports. A user self-service portal is also given.

Why worth watching: AppTec360 provides its regional servers in Germany and Switzerland, focusing on data security with a worldwide presence.

BlackBerry

BlackBerry has a long history in wireless devices and other solutions in the mobile communication market. Since then, BlackBerry has provided a UEM solution and acquired Cylance in 2019 to provide AI-driven endpoint protection, detection, and response capabilities to enhance its endpoint security. Founded in 1984, BlackBerry has headquarters in Waterloo, Ontario, Canada, and operates worldwide.

BlackBerry UEM provides a single solution for device, application, and data management. BlackBerry UEM allows for control policies for users, devices, and applications visibility within a centralized console. Support for endpoint environments includes Android, iOS, macOS, Windows, and Chrome. Both on-premises and cloud deployment options are also given.

Why worth watching: Blackberry continues to provide an enterprise-grade UEM solution with endpoint protection, detection, and response capabilities.

Bravura Software

Bravura Software, based in Redmond, Washington, United States, offers its cloud based OptiTune solution. OptiTune provides endpoint inventory and protection, patch management, automated application deployment, with monitoring and alerting capabilities.

Why worth watching: Bravura Software is a growing endpoint management solution for SMBs in the United States.

Codeproof

Codeproof is a private company based in Sunnyvale, California, United States. It provides a SaaS-based mobile security solution to SMBs. The Codeproof Platform supports Apple, Android, and Microsoft endpoint devices. It also offers application distribution and configuration with app whitelisting and blacklisting capabilities. MDM enrollment is provided along with the ability to maintain privacy and containerization on BYOD devices. The solution also offers HIPPA, GDPR, and ELC compliance of protected endpoints.

Why worth watching: Codeproof provides a SaaS-based mobile security solution to SMBs that also helps to keep endpoints compliant with various laws, mandates, and regulations.

HCL BigFix

BigFix was founded in 1997 and was formally owned by IBM until HCL Technologies acquired it in 2019. BigFix is based in Emeryville, California, with offices globally, and offers endpoint management through a suite of products that includes Patch, Lifecycle, Compliance, Inventory, Insights, and Mobile capabilities.

HCL BigFix has a presence in North America and other world regions with good product support and professional services. HCL BigFix is a consideration for organizations requiring a single solution for servers, desktops, and mobile with strong patch management and automation, along with endpoint device and application management.

Why worth watching: HCL BigFix continues to build on its Zero Trust Security platform offering continuous monitoring and compliance of endpoints.

SOTI

Founded in 1995, SOTI is a large enterprise headquartered in Mississauga, Canada, with worldwide offices in the EMEA and APAC regions. SOTI has had a long-time product focus on MDM, EMM, and UEM solutions. Although past strategic direction focused on business

mobility and the Internet of Things (IoT) in 2017 with their SOTI ONE Platform, they have built onto its platform with SOTI Identity that provides centralized user authentication, single sign-on, and role management to its portfolio and SOTI Central giving an online community for SOTI partners and customers.

The SOTI ONE Platform is a tightly integrated set of products such as SOTI MobiControl, SOTI Connect, SOTI Identity, and SOTI XSight. MobiControl provides the mobility lifecycle management of endpoint devices. SOTI Connect focuses on the lifecycle management of an organization's mobile and industrial printers. SOTI Identity gives secure access to the SOTI ONE Platform suite of solutions. XSight provides analytics-based insights, support, and management tools to address mobile device problems.

Why worth watching: SOTI continues to expand its SOTI platform offering more capabilities to its customers.

Tanium

Tanium, founded in 2007, is a large company headquartered in Kirkland, Washington, with additional offices globally. Tanium has a large customer base in the EMEA region and deployments within branches of the U.S. Armed Forces, financial institutions, and retailers. The Tanium XEM Platform provides a range of capabilities such as asset, risk and compliance management, digital employee experience, and endpoint management.

Tanium's Endpoint Management is a solution of the Tanium XEM Platform that allows for the automated management of endpoints. It is capable of scanning and collecting endpoint details, monitoring end-user performance, as well as the ability to view and validate endpoint applications through a single set of policies.

Why worth watching: Tanium continues to grow its endpoint management solution enhanced by other capabilities within its Tanium XEM Platform.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e. a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack in global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors, because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are

- | | |
|-----------------|---|
| Strong positive | Outstanding support for the subject area, e.g. product functionality, or outstanding position of the company for financial stability. |
| Positive | Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this |

can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

- | | |
|----------|---|
| Neutral | Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence. |
| Weak | Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem. |
| Critical | Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers. |

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The target is providing a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors to Watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

[Executive View: IBM MaaS360 with Watson - 79067](#)

[Executive View: ManageEngine Log360 - 80141](#)

[Executive View: ManageEngine PAM360 - 80140](#)

[Executive View: Microsoft Enterprise Mobility + Security Suite - 72541](#)

[Executive View: Sophos Intercept X - 80227](#)

[Leadership Compass: Access Management 2022 - 80757](#)

[Leadership Compass: Data Leakage Prevention - 80915](#)

[Leadership Compass: Endpoint Protection, Detection & Response - 80491](#)

[Leadership Compass: SASE Integration Suites - 81112](#)

[Leadership Compass: Security Orchestration Automation and Response \(SOAR\) - 80763](#)

[Leadership Compass: Zero Trust Network Access - 80474](#)

[Market Compass: Cybersecurity for Industrial Control Systems - 80913](#)

[Market Compass: Digital Workplace Delivery Platforms - 80475](#)

Copyright

©2023 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.