OMDIA

MARKET RADAR

Publication date
November 18, 2021

Author
Adam Holtby
Principal Analyst

Unified Endpoint Management Solutions, 2021–22

OMDIA

Brought to you by Informa Tech

Summary

Catalyst

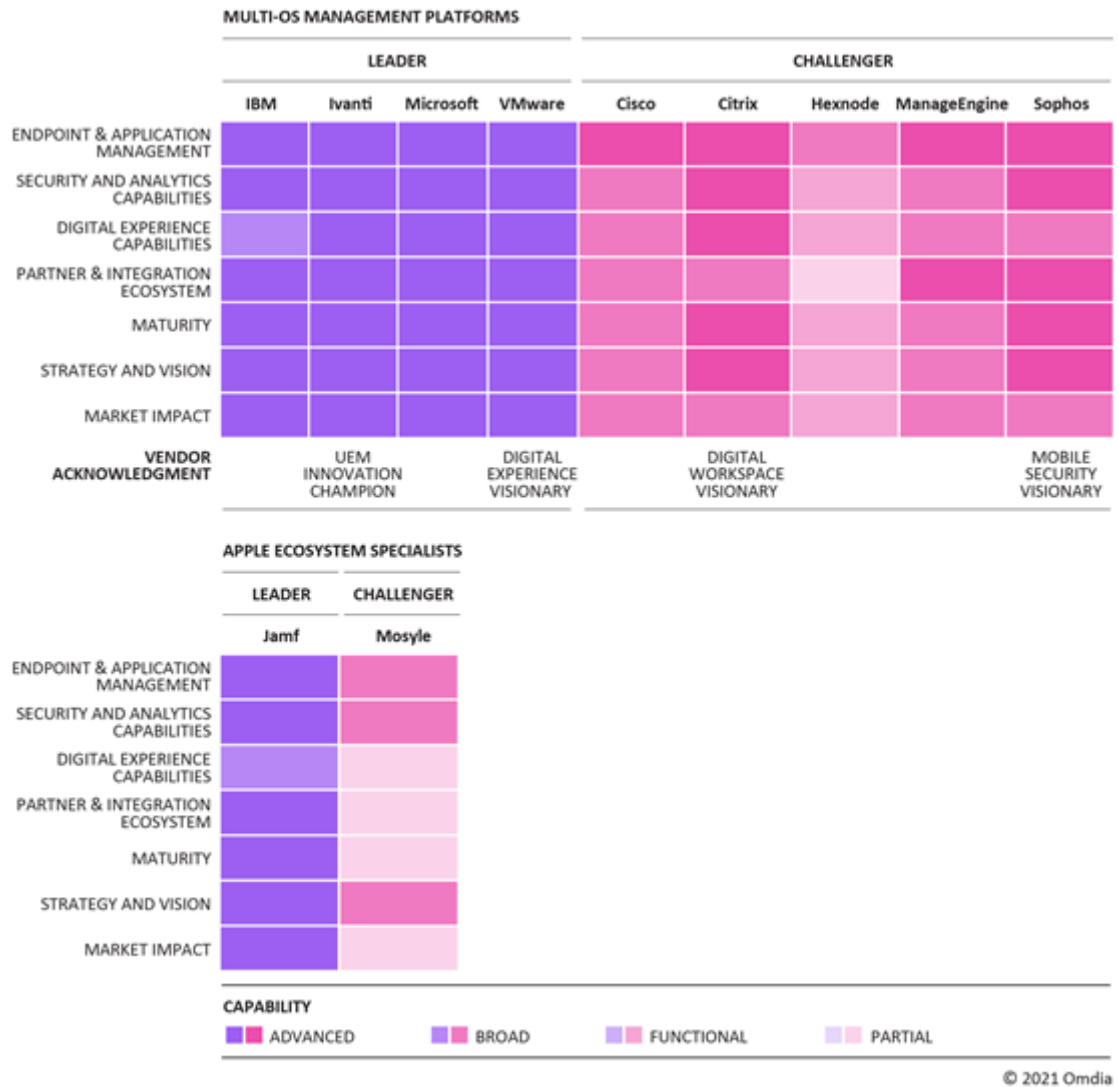
In this Market Radar, Omdia explores the Unified Endpoint Management (UEM) market and compares different solutions in this category. As work increasingly moves away from the traditional office, businesses are attaching great importance to UEM solutions that help manage and secure a more hybrid workforce. Organizations looking to embrace more modern management practices are driving growth in the UEM market and are positioning UEM solutions as a vital piece of the broader enterprise IT infrastructure puzzle.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Market snapshot

Figure 1 illustrates the solutions Omdia explored as part of this research, in addition to the highlighting capability categories analyzed. In addition to multi-OS management platforms, Omdia also explored UEM solutions that have a specialized Apple ecosystem focus. The definitions, assessment process, and vendor information is described in more detail later in this report.

Figure 1: Omdia vendor overview for Unified Endpoint Management solutions



Source: Omdia

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Key messages

- UEM capabilities and modern mobility management approaches are vital for organizations looking to better enable and secure a more hybrid and mobile-first workforce. The sudden shift to more mobile work styles brought about by the pandemic has resulted in businesses across the globe making long-term infrastructure and operational changes to support greater levels of hybrid work over the long term. Simplifying and unifying how the different endpoints and applications employees use can be managed and secured has become a vital digital objective for organizations.

- The need to better secure and manage mobile work styles, coupled with a need to improve employee experiences, are the key themes driving interest in UEM solutions. The value of UEM solutions beyond just the traditional mobile buyer is becoming better understood as businesses look to strengthen security and better influence and measure employee experiences. Mobile and security strategies are becoming more integrated, as are the internal business functions responsible for delivering them. Digital employee experience management (DEEM) capabilities are a compelling set of new capabilities that are increasingly being introduced by some UEM vendors.

- UEM solutions are a vital part of the broader digital workplace offerings service providers, and technology vendors are increasingly delivering. Omdia believes that a truly digital workplace is an ecosystem of different technical and service capabilities, as opposed to being one single “thing” or technology. UEM and mobility management solutions and infrastructure, alongside other tools and services including enterprise communication, customer engagement, and digital employee experience capabilities, are other important elements.

- A focus on people, processes, and technology has never been more important. In overcoming the challenges brought about by the pandemic, organizations must strategize and make investments that focus on optimizing the value from people, processes, and technologies, as well as reinventing their former business model. This is by no means a new mandate, but it has become an imperative due to the scale and speed of the technological, process, and people-centric changes and opportunities businesses now face. UEM capabilities have an important role to play in improving these areas.

© 2021 Omdia.
All rights reserved. Unauthorized
reproduction prohibited.

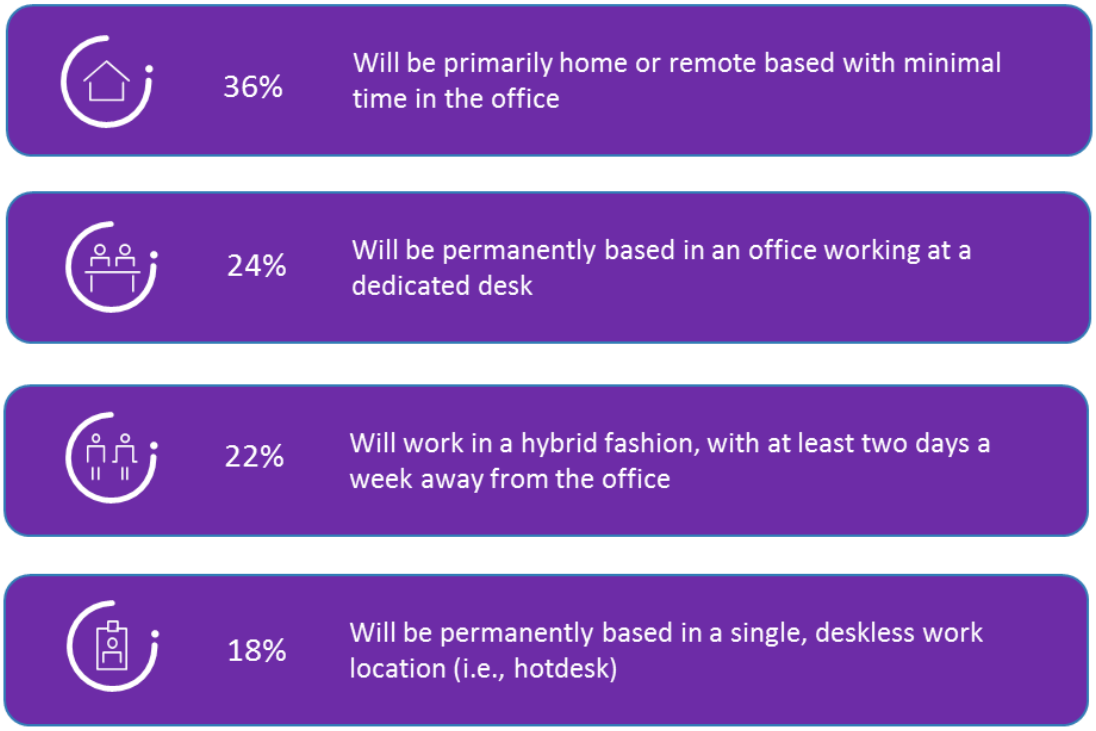
Omdia view

In Omdia's 2021 Future of Work survey, most enterprises identified UEM as being their most important workplace mobility objective. As long-term work styles for millions of people around the world have changed so dramatically in response to the pandemic, the appeal of a more modern and mobile-first endpoint and application management approach that is supported by UEM has greatly increased. Whilst not an especially new digital objective, the priority businesses are now attaching to adopting UEM solutions and practices that help secure and enable a more mobile workforce has never been greater. There are two key business needs driving interest in UEM: the demand to modernize and improve the way a mobile workforce is secured and managed, and the need to transform the process and workflows that shape the way that a more mobile-centric employee-base works.

While organizations continue to debate where employees will work as restrictions ease, our data shows that most businesses are planning for more work to take place away from the traditional office environment over the long term. Our 2021 Future of Work survey also showed that 58% of employees will either be primarily home-based or will adopt a hybrid work style going forward, as shown in **Figure 2:**

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Figure 2: More employees are set to work away from the traditional office



Source: Omdia

When enabling a hybrid workforce, businesses face a diverse set of people and technical challenges. Enterprise conversations and focus must now switch away from the locations that employees work from; businesses should plan to create an infrastructure and invest in solutions that support more modern work styles where employees can work from wherever they need to and with no compromises to security or productivity. UEM capabilities help improve the way that a more mobile workforce is managed and secured, regardless of if employees are working in the traditional office or on the move. These capabilities, coupled with how UEM helps modernize more traditional end-user computing approaches, have made them an important digital capability.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Recommendations

Recommendations for enterprises

- Strengthening security is a key UEM value proposition, but the importance of these tools to improve employee experiences should not be overlooked. Enterprises should work with vendors that offer capabilities and services that not only help strengthen security and mobility management practices, but that also provide features that help businesses transform the way mobile work gets done. Workflow automation, mobile reporting and analytics, and identity management capabilities are all important examples here.
- The mobile security, identity, and policy management capabilities offered by UEM solutions make them an important investment for organizations looking to embrace a zero-trust security approach.
- In addition to numerous UEM tools and platforms that offer some level of support for different endpoints and OSs, more specialized tools developed to cater to the needs of organizations invested in specific ecosystems, including Apple and Google Chrome, also exist. Organizations well invested in the Apple ecosystem should consider these specialized tools in addition to the multi-OS platform offerings and invest in a solution that offers a comprehensive and robust feature set that will help them manage, secure, and enable their employees.

Recommendations for technology vendors

- Technology vendor go-to-market (GTM) activities must advocate and market the value not only of the endpoint management and security capabilities offered by UEM tools, but also of how these solutions help businesses aggregate data across the different devices, apps, user behaviors, and connectivity solutions used. This level of intelligence provides many strategic insights that businesses can use as part of continual improvement and reporting activities.
- Verticalization of UEM solutions will be important in helping reduce complexities associated with adoption, and with workplace mobility programs more generally. Enterprises across different industries are interested in solutions that are tailored specifically to their industry and digital needs, so productizing around these is something UEM vendors should look to do. Healthcare, manufacturing, retail, and telecoms are areas of particular importance.
- Persona-based mobility solutions will also be important going forward, with frontline workers being of particular interest. As the use of digital and mobile capabilities increases amongst frontline workers, UEM solutions can play an important role in securing and managing this work.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Recommendations for service providers

- Service providers must leverage UEM capabilities as a vital component of their broader enterprise security and digital workspace service offerings. Delivering services that tightly integrate UEM with other enterprise-IT products, including mobile security management (MSM) and enterprise communications capabilities, will help reduce the enterprise mobile complexities that businesses face. The rise in hybrid work means enterprises have new demand for compelling mobile connectivity, management and security, and productivity capabilities. Service providers that have this holistic view of mobility and provide services that combine these capabilities will have strong appeal amongst mid-to-large-sized organizations looking to mature their hybrid and mobile-first work programs.

- Service management capabilities are becoming an important element of the mobility management services offered by some service providers. By integrating service management and UEM capabilities, service providers can improve the B2B services they deliver. By integrating these capabilities and through eBonding service management capabilities with those of their customers, service providers such as Orange Business Services and Vodafone have created compelling managed mobility propositions. These services are helping businesses improve activities, including device/app provisioning and user support, whilst also helping businesses digitize and automate important workflows.

- The UEM market is comprised of solutions that are designed to support multi-OS environments and tools that have been specifically developed to cater to specific OS ecosystems, including Apple and ChromeOS/Android. In ensuring their mobility services meet the needs of organizations that have more specialized mobility management requirements, service providers must establish partnerships not only with providers of multi-OS UEM solutions (Microsoft, VMware, IBM, etc.) but also with more specialized UEM providers (Jamf, Google, Mosyle, etc.).

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Defining the unified endpoint management market

Definition and characteristics

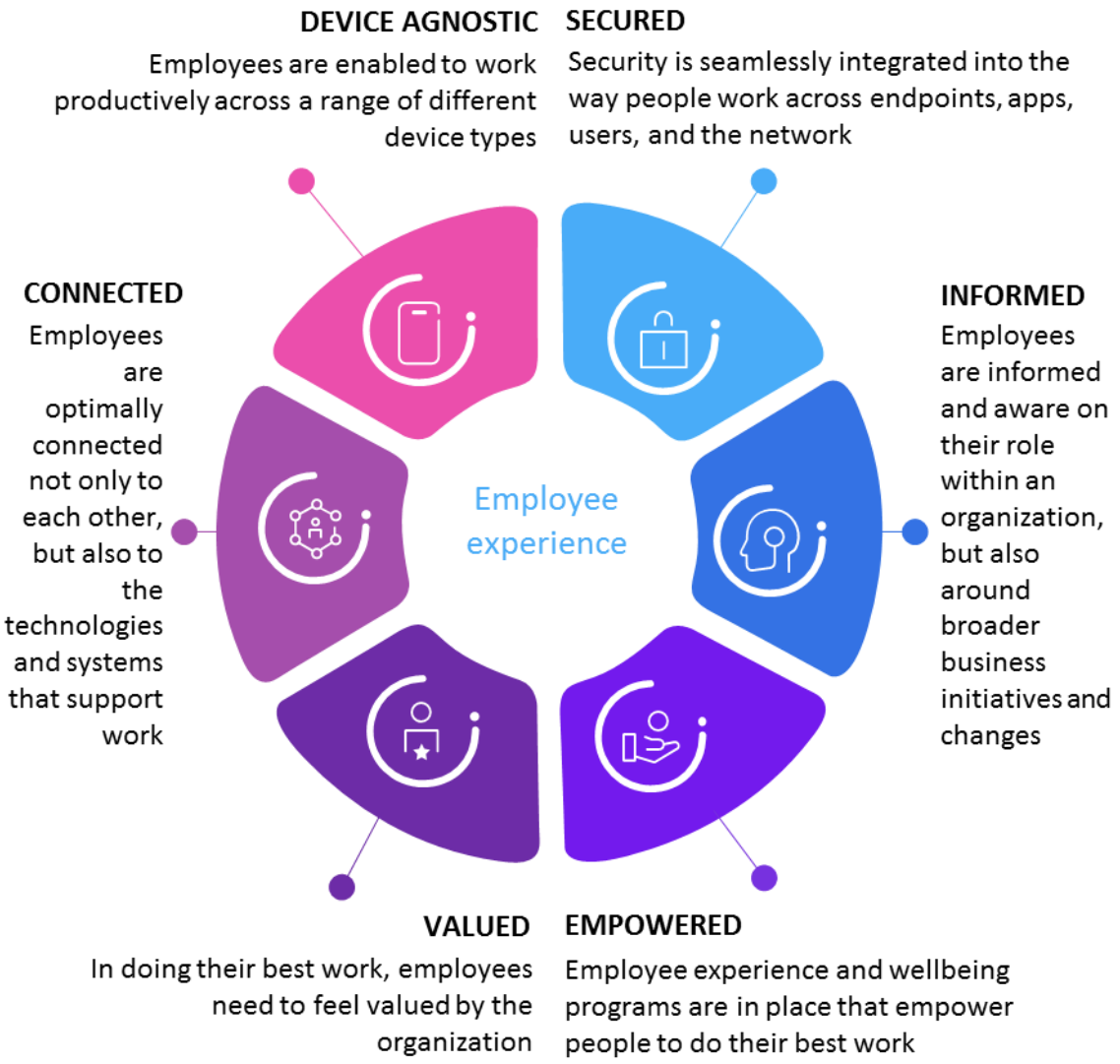
UEM solutions enable businesses to secure and manage the diverse range of devices and applications that are now used by employees. Traditional mobile devices (such as laptops and smartphones) and desktops and laptops running OSs such as Windows and macOS, and increasingly, other device types such as wearables, IoT devices, and even vehicles can be managed via these solutions. Increasingly, UEM tools are also being used to help businesses better measure and manage the experiences employees have with digital technologies. UEM is best thought of as an evolution of the enterprise mobility management (EMM) and mobile device management (MDM) tools that came before. The added value offered by UEM solutions is built around how the solutions support businesses looking to manage a broader estate of device and OS types, the enhanced endpoint security and analytics capabilities offered by these platforms, and features that help employees work in a more productive and engaging way. Additionally, and with businesses' focus on security issues increasing, UEM technologies deliver attractive capabilities that support efforts around zero-trust security approaches.

UEM is more than just an integration of what have traditionally been point-based endpoint management technologies. It is important that the migration to a more unified endpoint management approach considers more than just the technology. For years, the teams and means responsible for managing mobile devices and those responsible for managing traditional endpoints and client PCs have been separate. UEM should not only unify the capabilities these teams use in managing and securing the end-user-computing (EUC) estate; it should also act as a catalyst to developing better synergy and working practices between the mobility management and traditional endpoint/client management teams. Formally merging teams where separate is an approach that many businesses are now embracing because this helps in delivering a more consistent approach to EUC. Improving employee productivity and experiences and supporting more modern, often mobile approaches to work should be the overarching business objectives guiding this integration effort.

UEM solutions help businesses make hybrid work a reality by securing and managing a more mobile workforce, helping organizations support a set of important workforce characteristics that help empower and enable employees to do their best work. Omdia views UEM as a vital digital workplace capability that helps organizations to better enable and empower a more hybrid and mobile-first workforce, as shown in **Figure 3:**

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Figure 3: The hybrid workforce



Source: Omdia

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Key capabilities and vendor landscape

As demand from enterprises to better secure and manage a mobile workforce has increased against the backdrop of the pandemic, interest in UEM solutions has accelerated. The market is very competitive, embodying solutions from a range of different platform-focused and specialist technology providers that serve the needs of different size global organizations. These providers offer a diverse set of capabilities that help businesses manage and secure the range of OSs now used across the different devices that employees interact with. The concept of UEM is now also much better understood, evidenced by results from Omdia's 2021 *Future of Work* survey that highlighted how most of the enterprises surveyed view UEM as being the most important workplace mobility priority. Service providers also play an important role in this market, delivering UEM capabilities as part of their broader digital workplace and managed mobility service offerings. As workplace mobility programs can be complex, the services that have UEM capabilities at their core will be viewed by enterprises as important, especially in helping them navigate the many management, security, and connectivity complexities they experience.

From a technical perspective, the endpoint and application management capabilities enterprises have come to expect from a UEM tool remain at the core of these solutions and are key in driving interest and adoption of these solutions. UEM platforms that offer a broad range of management and security capabilities from the likes of Microsoft, VMware, and IBM still dominate the market in terms of overall adoption, but providers of specialist capabilities—such as Jamf that supports the needs of an iOS end-user ecosystem—are also experiencing good traction. The likes of Ivanti, Citrix, and Cisco are also aiming to differentiate in interesting ways by building on their core mobile endpoint management propositions with new security, employee productivity, and digital workspace capabilities. Capabilities that help enterprises measure and positively impact the employee experience across mobile are also important, as are AI and workflow automation features that are being used to help improve reporting, compliance, and the security of a mobile workforce.

In developing this research, Omdia assessed different UEM solutions and vendor capabilities across a range of different criteria, as shown in **Figure 4:**

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Figure 4: UEM market radar capabilities

Endpoint and application management	Capabilities offered that enable businesses to manage, configure, and monitor a broad variety of endpoints, OSs, and mobile apps
Security and analytics	Advanced security and analytics features, including conditional access and device and app insights powered by AI
Digital experience	Features such as mobile workflow capabilities and self-service capabilities that help improve the employee experience for the mobile workforce
Integration and partner ecosystem	Ability to integrate with other enterprise systems in addition to an assessment of partnerships the vendor has in place with service providers
Maturity	Maturity of solution based on elements such as adoption patterns, support practices in place, and additional services available
Strategy and vision	Analysis into vendor roadmap and plans for solution going forward, and consideration of solution differentiation
Market impact	Impact of solution on the UEM market based on elements including revenue and growth, geographical penetration, and interest in solution based on enquiries

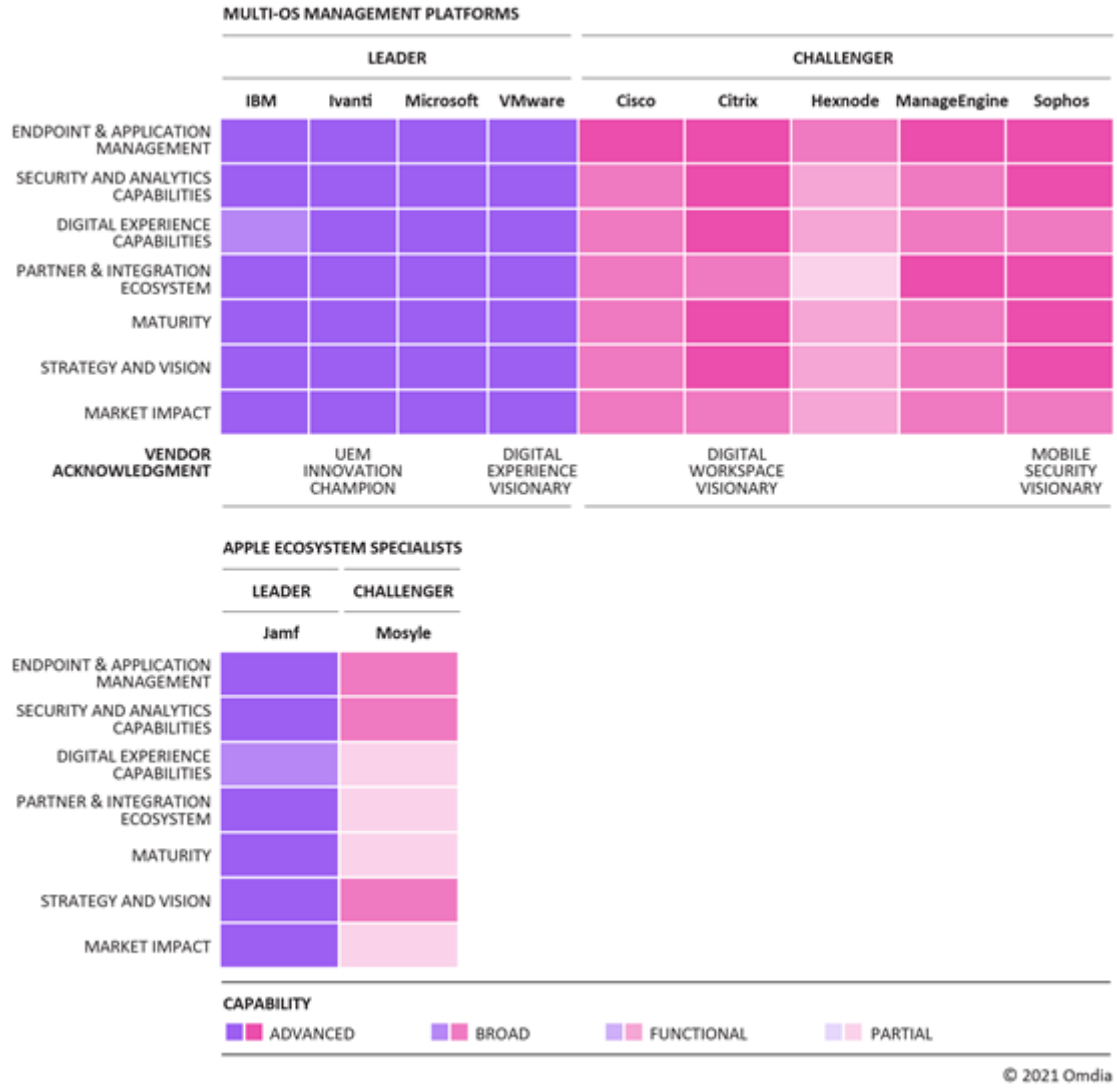
© 2021 Omdia

Source: Omdia

All of the vendors covered in this report offer a robust set of features and a balanced portfolio of capabilities that can be customized to the requirements of the enterprise sector, and **Figure 5** illustrates the capabilities delivered by the competing UEM offerings that Omdia analyzed for this research. Additionally, the vendors we explored in this research offer solutions across all major geographies and have traction with and a strategy to target mid-to-large-sized organizations. We have also (for the first time) explored specialist solutions that, by design, have been developed to support businesses heavily invested in the Apple ecosystem.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Figure 5: Omdia heatmap for UEM solutions



Source: Omdia

The Omdia Heatmap for UEM solutions is colored as follows:

- **Advanced capability:** The vendor demonstrates very strong capabilities and/or capability in alignment with what Omdia explored as part of this research.
- **Broad capability:** The vendor offers better-than-expected capabilities that are well-suited to the needs of most businesses.
- **Partial capability:** The vendor provides expected capability but lacks some of the advanced capabilities assessed as part of this research.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

- **Limited capability:** The vendor provides limited, or none of the expected capability explored as part of this category

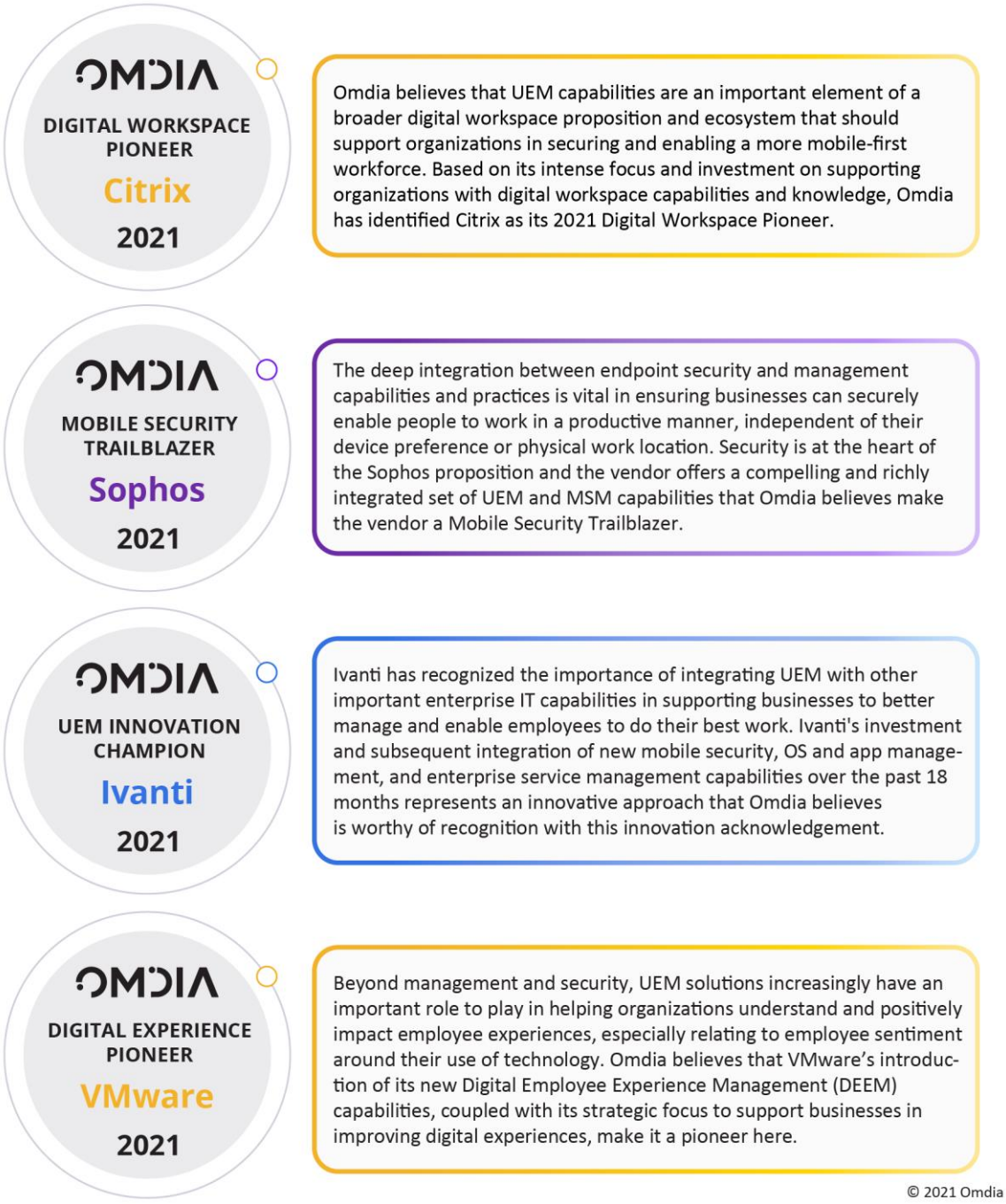
The categorization of each vendor is as follows:

- **Market leader:** This category represents the leading solutions that provide advanced capabilities across six or more areas explored and which we believe are worthy of a place on most technology selection shortlists.
- **Market challenger:** The solutions in this category offer some advanced or broad capabilities, have appropriate functionality across other areas and should be considered as part of a technology selection process.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Vendor acknowledgments

The vendor heatmap provides an important perspective of the comprehensiveness and relative strengths of each vendor's solution. In addition to this evaluation, Omdia has also acknowledged a selection of vendors that it believes, based on capability and strategic analysis, have demonstrated progress and success against the categories identified below:

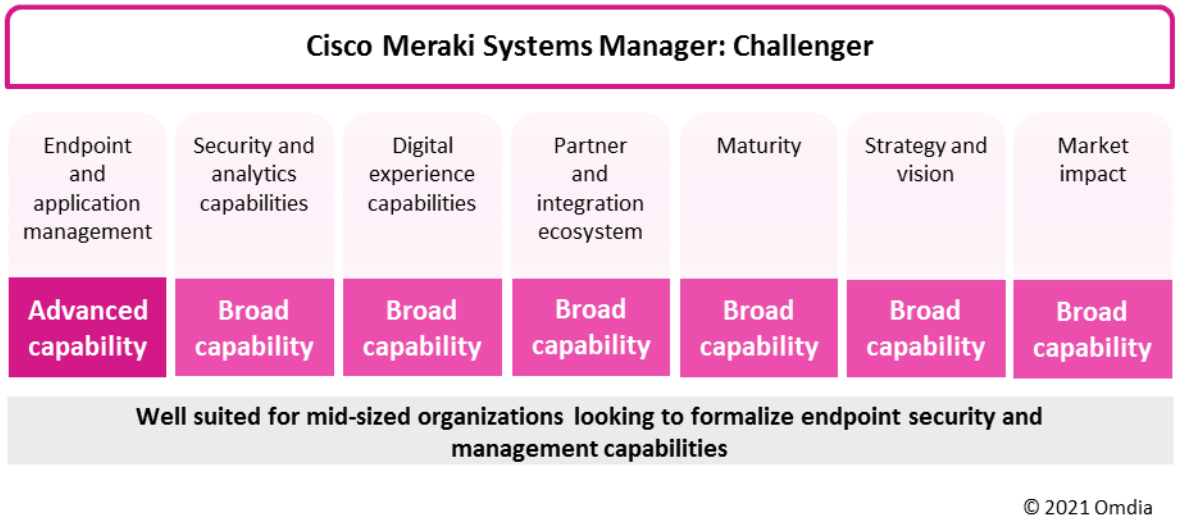


© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Vendor Analysis

Cisco Meraki Systems Manager

Figure 6: Omdia Market Radar recommendation—Cisco Meraki Systems Manager



Source: Omdia

Why consider Cisco Meraki Systems Manager?

- Cisco offers a strong set of core endpoint management features that are well suited towards supporting small to mid-sized organizations looking to better secure and manage employees across different devices and OSs, including iOS, Android, Windows, ChromeOS, and macOS.

- Cisco has a strong network heritage, something it leverages as part of its Systems Manager solution via its “Sentry” features. These features allow for automatic provisioning of Wi-Fi and VPN credentials for Meraki networks. Additionally, security can be strengthened with this capability by enforcing network policy rules based on device posture. Cisco Meraki provides a single cloud-managed console for both endpoint management and the network stack, helping make the management and admin of these important infrastructure components more streamlined. The broader Cisco security product suite offers endpoint security solutions, including DUO (identity management), Umbrella (DNS-layer web content filtering), AMP (malware detection/protection), and ISE (network access control). Systems Manager has rich integration with these products enabling customers to seamlessly deploy and configure these solutions across endpoint devices.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

- Systems Manager is a quality, affordable option for organizations already invested in the Cisco Meraki ecosystem. The solution offers a set of critical mobile and app management and security capabilities that are important for organizations looking to better enable a more hybrid and mobile workforce. Systems Manager should be a solution explored by Cisco Meraki customers that are just starting out on their UEM journey to improve how mobile devices and applications are managed and secured.

Roadmap and areas of future focus

- An important strategic focus for Cisco is to position Meraki Systems Manager as a tool to help organizations secure a more mobile workforce. As a result, a "Zero Trust" security paradigm will become a key focus area for the company as it starts to see customers adjust their endpoint management strategy to accommodate more flexible remote and hybrid worker use cases.

- Cisco Meraki Systems Manager does not currently deliver the breadth of capabilities offered by some other solutions in this market. Meraki Systems Manager is more a tool suited to SMEs or organizations already invested in the Meraki ecosystem. To raise appeal amongst enterprises and to better compete with the likes of VMware, IBM, and Microsoft, Cisco would need to further enhance its UEM proposition and capabilities.

- Improving the breadth and ease of integrations that Systems Manager has with other digital workplace capabilities is also an area Cisco should look to explore. Specifically, developing integrations with other third-party security solutions would be useful in delivering even greater security insights and controls to customers. Additionally, offering some way to measure and report on employee experiences, particularly relating to the mobile worker, would be useful and is something that other UEM vendors are investing quite heavily in.

Market impact

- Cisco Meraki Systems Manager is deployed as a software as a service (SaaS) solution only. The solution is licensed solely on a per-device basis—there is currently no per-user license option. Systems Manager is adopted by organizations across all major geographies, and Cisco has a global sales function and partner strategy that enables different routes to market.

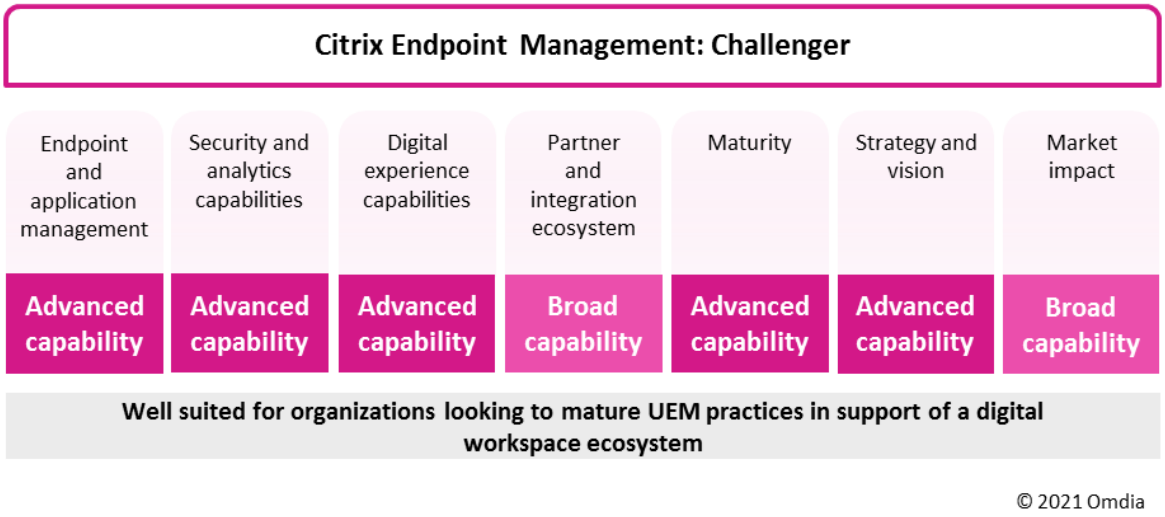
- Customers are positive about Meraki Systems Manager's app and device management capabilities and how the solution is affordable and easy to use. Additionally, customers are positive about the device provisioning and mobile insights and information the solution delivers.

- Cisco offers a comprehensive range of well-adopted enterprise IT solutions, giving the vendor a solid enterprise footprint. Cross-selling its UEM capabilities to customers that utilize other Cisco solutions is a good approach and is one that will help the vendor further increase its market traction. Network and endpoint security and management are important digital objectives that will help grow interest in an integrated solution such as Cisco's.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Citrix Endpoint Management

Figure 7: Omdia Market Radar recommendation—Citrix Endpoint Management



Source: Omdia

Why consider Citrix?

- Citrix Endpoint Management is a key part of Citrix's broader digital workspace solution that helps businesses streamline access to important applications, collaborate and share business information and data, and improve and virtualize access to important work resources. Citrix Endpoint Management helps organizations improve the management and security of different mobile and traditional OSs. Citrix has deeply integrated a strong set of mobile security capabilities and practices—most notably around zero-trust access—into its endpoint management offering.

- Citrix has a focus on helping businesses improve employee experiences through its endpoint management and digital workspace solutions. The vendor achieves this through offering capabilities that help businesses optimize important processes like employee onboarding, streamlining device administration and management activities, and simplifying the technology experience for employees. Employee experience is becoming a critical objective for organizations, so this focus from Citrix is important. Citrix also offers a support and rating system for all UEM-delivered applications to help admins better understand what end-user difficulties are being experienced at an app-level. To support the adoption of its technology, Citrix also offers services that have been developed to strategically support customers in maximizing their return on investment. Citrix's Customer Success Services are focused on ensuring deployments are successful and continue to deliver key value for customers over the long term. In supporting a more service-led approach, Citrix recently announced fundamental changes to its executive leadership team, with all sales and customer service

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

teams now reporting to a customer officer. This change was made to strengthen Citrix's customer-centric approach throughout the entire lifecycle of any engagement.

- Citrix has a strong relationship and integration with Microsoft's Endpoint Management capabilities, something that is important given Microsoft's ongoing success in this space. The integrated set of capabilities delivered provide additional security and productivity benefits to both Microsoft Endpoint Manager and Citrix Endpoint Management customers.

Roadmap and areas of future focus

- Citrix's endpoint management capabilities currently have strong appeal with organizations already invested in the Citrix ecosystem. Given the priority that many organizations are now attaching to securing a more mobile and hybrid workforce, there is an opportunity for Citrix to raise the appeal and improve the adoption of its endpoint management capabilities with new customers that do not currently work with the vendor.

- The concept of the digital workspace is becoming better understood by enterprises and the market at large, and Citrix intends to keep building out its native capabilities here, in addition to further strengthening its partner ecosystem and third-party integrations. This will be important given that a true digital workspace is more an ecosystem of different technology and service capabilities that need to be richly integrated into supporting important digital priorities.

- Better measuring and being able to shape employee experiences, particularly in their use of digital tools, is becoming an important objective for organizations. Citrix should explore investment in new digital employee experience management capabilities to further enhance its UEM proposition.

Market impact

- Citrix creates and delivers UEM solutions across different industry verticals and provides dedicated industry services in support of its approach here. Citrix Endpoint Management is currently well adopted by businesses across government, healthcare, financial services, technology, and professional service verticals.

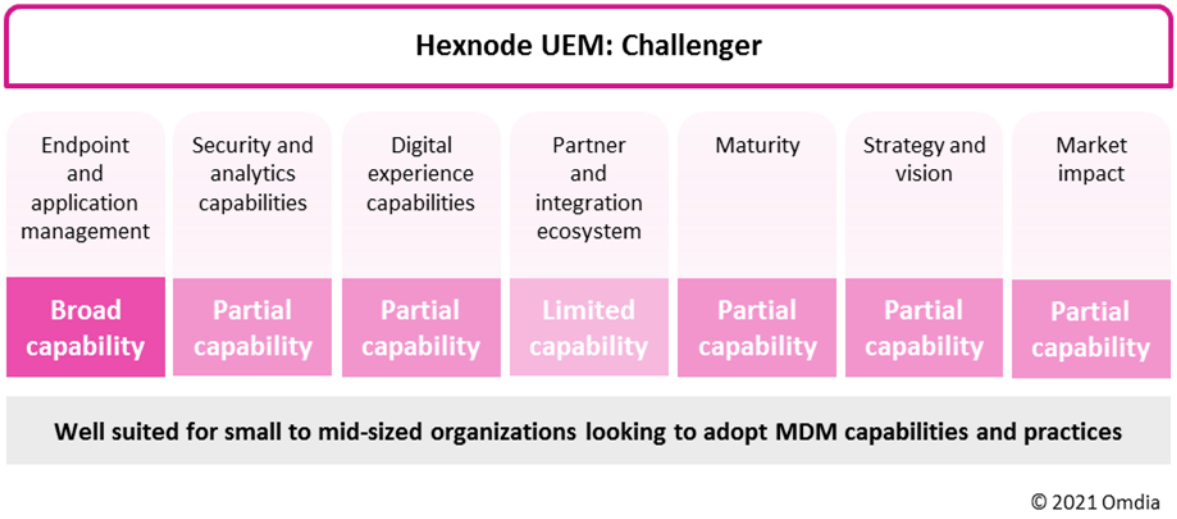
- The solution has strong adoption amongst North American and European organizations of different sizes. Citrix has good adoption amongst larger organizations (5,000+ employees), and the vendor is looking to grow traction amongst these larger enterprises further.

- Driven by the increased demand and prioritization that organizations have around mobility management and security solutions, Citrix reports strong revenue associated with its UEM product over the last financial year. While Omdia does not currently see Citrix's UEM proposition as having the broad market mindshare and awareness shared by some of its peers in this space, its strong capabilities make it a solution that will meet the needs of businesses of different sizes and mobility management maturity.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Hexnode UEM

Figure 8: Omdia Market Radar recommendation—Hexnode UEM



Source: Omdia

Why consider Hexnode?

- Hexnode is a new entrant to this year's UEM market radar. The vendor offers a good set of core device management features that support organizations in provisioning and securing a range of different endpoints, including Windows, Android, and iOS devices. Devices can be enrolled in bulk, and via a zero-touch approach preconfigured with the applications needed by employees. Hexnode offers a good set of device policy management features, including the ability to define and enforce device security policies based on geofencing. Administrators can define different device configurations based on location.

- Customers are positive about the Hexnode user interface, particularly around how it is simple to use and easy to navigate and work with. Hexnode offers remote management capabilities that enable customers to undertake remote support actions on devices. Support can also be delivered via a messenger capability—functionality that can further support businesses in improving the user experience and employee support.

- Hexnode also offers a certification program in its Hexnode Academy. The program and curriculum have been developed to support and educate customers around the Hexnode solution and UEM best practices in general. As the transition from more traditional client and endpoint management approaches to UEM can be challenging, educational resources and programs like this can be valuable in supporting adoption and in enhancing employee mobility management and security digital skills.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Roadmap and areas of future focus

- Hexnode offers a good set of core MDM capabilities and is a solution that currently has appeal amongst small to mid-sized organizations. However, Hexnode does not currently offer the same level of broader and more advanced UEM capabilities delivered by most of the more well-established solutions in this space. To increase appeal amongst larger organizations in particular, Hexnode will need to expand the capabilities offered by its UEM solution.

- Improving its MSM capabilities is in Hexnode's roadmap. Omdia is tracking a lot of business interest and investment in MSM (also known as mobile threat defense (MTD)), capabilities that support businesses in further maturing mobile security approaches. Some UEM vendors offer these capabilities natively, whilst others integrate with specialized solutions in this area. As these features become increasingly important in securing BYO environments, developing this integration will be important for UEM vendors such as Hexnode.

- Omdia has seen an increase in the adoption of Chromebooks during the pandemic, both within the education sector and beyond. Supporting businesses with ChromeOS management capabilities would be a good enhancement for Hexnode to make.

Market impact

- Hexnode's current appeal is more amongst small to mid-market organizations that are exploring the adoption of cloud-based MDM capabilities. The UEM market is a competitive one, so increasing its modest market share compared to its competitors will be difficult. In keeping pace with mid-market competitors, Hexnode must continue to introduce new mobile security capabilities in addition to features that help organizations improve the digital employee experience.

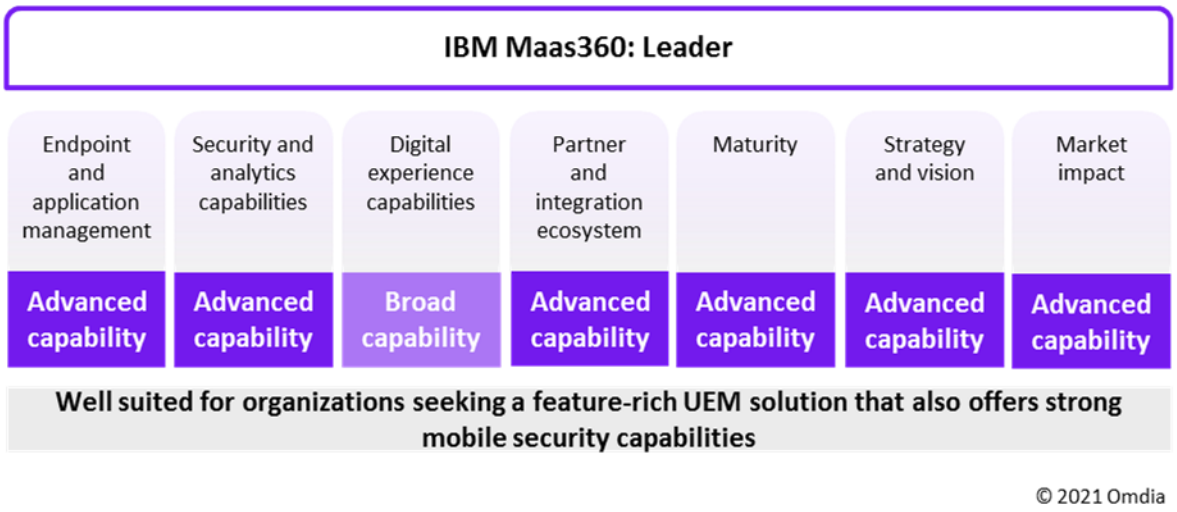
- Hexnode was founded in 2013, and the company is headquartered in San Francisco, California. Hexnode delivers UEM solutions to customers across all industries, including healthcare and financial services. Hexnode currently has a strong presence in North America, but also in Europe and the Middle East and Africa.

- Whilst Hexnode's partner ecosystem could be improved, the vendor does offer API integrations for partners wishing to integrate their capabilities into the Hexnode UEM solution. Hexnode recently announced a new Partner Relationship Management Portal that aims to make it easier for Hexnode to support its sales partners with marketing materials and order tracking capabilities. Growing its market awareness will be important for Hexnode, and developing its partner ecosystem with service integrators and managed service providers will help.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

IBM MaaS360

Figure 9: Omdia Market Radar recommendation—IBM MaaS360



Source: Omdia

Why consider IBM Maas360?

- IBM MaaS360 boasts a comprehensive set of UEM capabilities, with support for a diverse range of OSs that help organizations in the management of the many different devices that employees now use in the workplace. Beyond core endpoint management, MaaS360 empowers businesses with features that help gather device data and insights, including information on apps associated with a device. These insights provide admins with good visibility and control over how to fine-tune the mobile user experience.

- MaaS360's core endpoint management capabilities are supported by a strong set of mobile security features that IBM continues to invest in. MaaS360 has native malware detection capability (powered by Trusteer), and the solution also detects threats (such as phishing) on devices. For advanced threat detection, MaaS360 can leverage Wandera (now owned by Jamf)—a leader in MSM/MTD, according to Omdia's recent MSM report. MaaS360 supports native conditional access via IBM's built-in IAM capability (powered by IBM Security Verify). The solution also delivers two-factor authentication for customers out of the box. Beyond its native capabilities here, MaaS360 also integrates with third-party IDP (Azure AD, Ping, Okta) to support multifactor authentication and conditional access.

- IBM Watson's capabilities are richly integrated into Maas360, providing customers with actionable and cognitive insights that help improve how the mobile workforce is managed and secured. From a mobile security perspective, My Advisor with Watson provides customers with insights on vulnerability and OS risks based on their device fleet.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Additionally, MaaS360 has user risk analytics capabilities that help admins monitor user behavior anomalies across their device estate and quantify them in creating a risk score. This risk score can be used as part of a conditional access approach. Admins can monitor risk across all their users and devices over time to understand trends, top risk incidents, and to take appropriate corrective actions.

Roadmap and areas of future focus

- IBM's strong focus on security will see the vendor further invest in capabilities that support businesses looking to embrace zero-trust security methodologies. The mass move to hybrid working, and the long-term plans organizations have to embrace this work style permanently, is making security a huge area of interest and investment for enterprises. IBM plans to expand MaaS360's security features to detect and prevent data leakages and network threats, and by introducing capabilities that will further improve risk analytics and security dashboards.

- Microsoft's endpoint management solution poses a threat to MaaS360, as it does with other UEM solutions. Microsoft's strong and established enterprise presence, coupled with the affordability of its Endpoint Manager solution, make it an attractive UEM solution for many businesses. IBM must continue to market to organizations the value and importance of tools that offer a comprehensive set of management and security capabilities that extend beyond just the Microsoft and Office365 ecosystems.

- IBM MaaS360 is currently only available as a SaaS offering, which may limit the appeal of the solution amongst certain organizations who haven't made the move to the cloud. Whilst a cloud-based deployment model is currently the only option, IBM advises that a hybrid/hosted option is part of its roadmap.

Market impact

- Millions of iOS, Android, Windows 10, ChromeOS, and macOS devices are currently under management with MaaS360, with the two most popular device types under management being iOS and Android. The solution is licensed on both a per-device and per-user basis, with the per-device model being the most popular at present. Most organizations currently adopting IBM MaaS360 are based in North America. There is a lot of potential for IBM to grow adoption further in Europe and Asia & Oceania. MaaS360 has strong traction amongst mid-to-large sized organizations, and with manufacturing retail, professional services, and healthcare organizations.

- IBM boasts a very strong partner network, one that sees the majority of MaaS360 sales coming via channel partners. In particular, a very healthy share of sales is made via telco partners that will offer MaaS360 as part of their broader managed mobility offerings that combine UEM with connectivity and other security and productivity solutions. Telco providers are a key GTM partner for MaaS360, and the value-added services that are combined with MaaS360 by these partners in maximizing adoption and ROI is a key reason why. Another key aspect of IBM's GTM strategy is in leveraging digital marketplaces to simplify the sales processes and to automate the provisioning of the solution. IBM partners

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

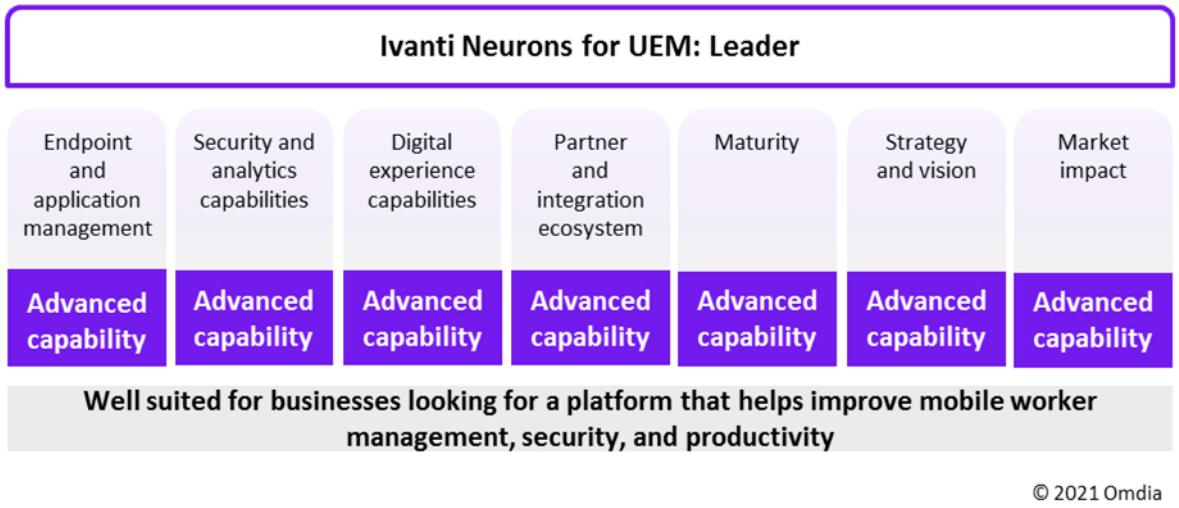
with multiple cloud marketplace vendors here, and it continues to expand its partners here. IBM MaaS360 also boasts a diverse range of rich integrations with numerous third-party enterprise technologies that help organizations deliver optimal employee experiences. MaaS360 has a robust API layer that allows partners to build value-added solutions by embedding MaaS360 into their offerings, as well as integrating with MaaS360 at a product-to-product level.

- Whilst IBM does not currently offer verticalized solutions targeted to specific industries, MaaS360 is currently adopted by organizations across numerous verticals and supports a variety of different use cases. IBM provides the capability for organizations to simplify workflows based on these use cases; for example, by providing policy templates and recommendations aligned with the needs of organizations with different security needs and priorities based on industry standards such as HIPAA, CJIS, GDPR, etc.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Ivanti Neurons for UEM

Figure 10: Omdia Market Radar recommendation—Ivanti Neurons for UEM



Source: Omdia

Why consider Ivanti Neurons for UEM?

- It has been a very eventful 18 months or so for Ivanti, with the vendor making a series of major acquisitions across different product categories that have significantly strengthened the vendor's overall value proposition. Notably, Ivanti's acquisitions and integration of MobileIron and Pulse Secure products with its own client management capabilities means that the vendor now offers a very capable and appealing UEM solution. The security and mobility management capabilities Ivanti now offers are further complimented by the strong service management and workflow automation capabilities the vendor also delivers. Collectively, these capabilities not only help organizations better manage and secure a more mobile workforce, but they also support efforts to modernize, digitize, and automate the workflows and processes that guide how work gets done.

- Richly integrating UEM with workflow automation and service management capabilities delivers many benefits for organizations. For example, Ivanti's discovery capabilities are supported by its strong service management proposition and provide organizations with the ability to identify unmanaged devices and services on a network. Once these devices and services have been discovered, Ivanti can secure them and bring them under management. The automation capabilities of Ivanti Neurons can also be leveraged to automatically take corrective actions against non-compliant devices without IT or user interventions. The creation of a common and single data source that extends across UEM, security, and enterprise service management that Ivanti now delivers enables businesses to better personalize services and to make more informed and contextualized business decisions.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

- Ivanti offers a very strong set of mobile and client security features, including integrated MTD, passwordless multi-factor authentication, and policy- and risk-based patch management. Ivanti also delivers features that help organizations improve employee experiences through the early detection, management, and remediation of employee issues attributed to things such as device and app performance.

Roadmap and areas of future focus

- When organizations make numerous acquisitions over a short space of time, especially across different product categories, it can take time until the new collective value proposition becomes better understood by the wider market. Ivanti now offers a very strong UEM solution, so educating and communicating its new collective capabilities to enterprises is currently an important activity for the organization. Engaging service provider partners will be important here, especially given the criticality of service management and mobile worker security solutions to the managed services and solutions these providers offer.

- Ivanti advises that its immediate strategic focus is in helping enterprises connect unified endpoint management, zero-trust security, and enterprise service management capabilities. The company is executing on its vision and strategy to deliver an intelligence-driven hyper-automation platform that helps organizations enable a more mobile workforce with self-heal, self-secure, and self-service capabilities from the cloud to the edge.

- Ivanti currently offers verticalized solutions that help tailor its capabilities to the specific needs and pain points of businesses across different industries, including supply chain and healthcare. Ivanti also supports a wide range of use cases for the management and security of devices used by frontline workers across healthcare, retail, services, manufacturing, and supply chain industries. This includes support for IoT devices, shared tablets used by nurses, BYO devices used by doctors, point-of-sale of kiosk devices in retail locations, tablets used by service technicians, and barcode scanners in warehouses, in addition to other special-purpose use-cases. This is a strategy and product development approach that Ivanti should continue with as it will help improve the adoption and understanding of its new platform offering.

Market impact

- Ivanti's recent acquisitions of MobileIron (UEM), Pulse Secure (network security), RiskSense (risk-based vulnerability management), and Cherwell (enterprise service management) have helped the vendor elevate its status and mature its UEM and broader enterprise IT proposition. Ivanti reports that within six months of acquiring MobileIron and Pulse Secure, it was able to deliver its integrated Ivanti Neurons Platform to market.

- Ivanti currently has a good mix of customers across different enterprise size bands. In Ivanti Neurons for UEM, it has a feature-rich UEM solution that also has the potential to help Ivanti grow adoption even further amongst larger enterprises (5K+ employees). The vendor also reports strong UEM-related revenue and good SaaS revenue growth across all major geographies over the past financial year.

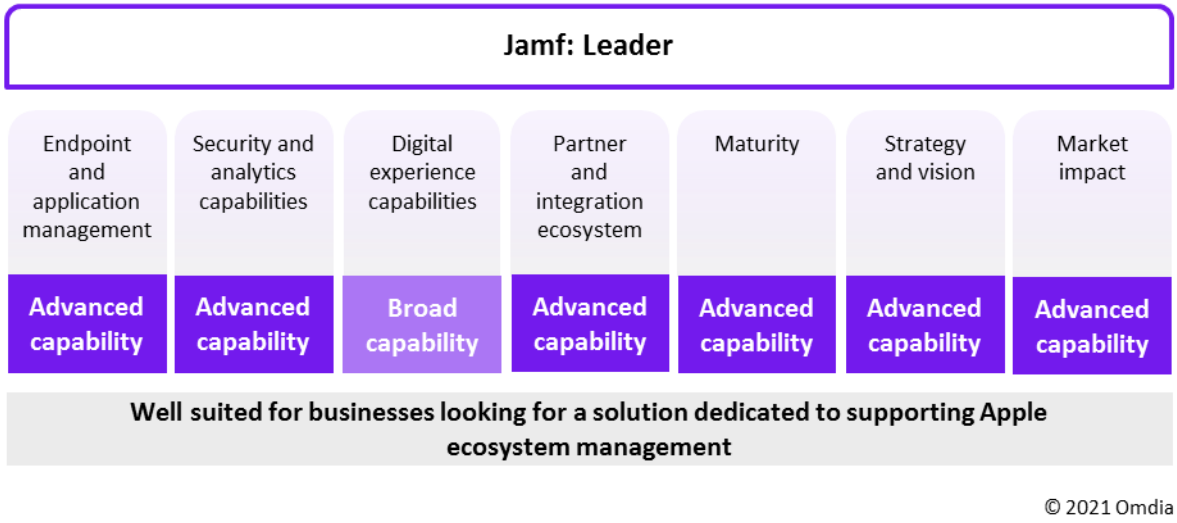
© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

- Ivanti's solutions are available via both on-premises and SaaS deployment models. Its routes to market are direct and through a diverse set of channel/VARs, OEM, carrier/telcos, and managed service provider (MSP) partners. Currently, the direct channel is the most popular for Ivanti, but the vendor is looking to further grow traction via telco and MSPs especially. This GTM strategy will be supported by Ivanti's ongoing efforts to verticalize its offerings.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Jamf

Figure 11: Omdia Market Radar recommendation—Jamf



Source: Omdia

Why consider Jamf?

- Jamf is a feature-rich UEM solution for organizations invested in the Apple ecosystem that rely on iOS and macOS devices in getting work done. As Jamf is, by design, a solution developed to support organizations in the management and security of Apple devices, the solution provides a specialized approach and capabilities aimed specifically at this need. Jamf has a close relationship with Apple, one that means its solution supports new Apple features and functionality the same day Apple ships their major OSs. Jamf's recent acquisition of MSM market leader Wandera is also notable as these capabilities significantly strengthen Jamf's overall security proposition, both within the Apple ecosystem and beyond.

- Jamf offers a comprehensive set of Apple endpoint and application management and security capabilities. For example, Jamf enables businesses to conduct comprehensive risk assessments of installed apps as part of security auditing. Additionally, Jamf also provides security compliance and benchmark enforcement capabilities for common standards that further support organizations' auditing and mobile security practices. Jamf is also supporting enterprise efforts to move to a zero-trust security model by leveraging data science to identify anomalies in traffic flows and by extending some data policy capabilities beyond the device and into the network. As previously mentioned, Jamf's recent acquisition of Wandera—an MSM/MTD solution that Omdia recently identified as a market leader—has also further strengthened its broader mobile security capabilities.

- Many of the organizations Jamf works with that offer both Apple and non-Apple products use Jamf's solution alongside other UEM tools—most commonly Microsoft Endpoint

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Manager—in delivering a comprehensive and unified end-user computing environment. Jamf has a multi-pronged integration with Microsoft that allows both platforms to run together harmoniously in any environment, allowing customers to benefit from features such as a single pane of glass admin and management portal, unified reporting, and multi-OS conditional access capabilities. Jamf's specialized Apple management and security capabilities complement Microsoft's strong and widely adopted multi-OS endpoint management capabilities well.

Roadmap and areas of future focus

- As Jamf is developed around the Apple ecosystem, it is not a solution that should be adopted by organizations looking for one single platform to manage a multi-OS environment. However, Jamf's focus and specialized iOS, macOS, and iPadOS management capabilities, coupled with the market-leading multi-OS security features it has brought on board via the Wandera acquisition, make it a solution that organizations with a fleet of Apple devices should certainly explore, even if adopted in conjunction with another multi-OS solution. Jamf has established partnerships with technology providers such as Microsoft and Okta to eliminate IT overhead when adopting best-of-breed, ecosystem-based solutions.

- An important strategic agenda item for Jamf going forward is in developing its platform approach and offering. The acquisition of Wandera is significant in how the integrated set of capabilities will raise the profile and appeal of Jamf with customers looking to better secure more mobile work styles. Evolving its market positioning and perception around this heightened value proposition, especially amongst organizations that may not be well invested in the Apple ecosystem, will be important for Jamf going forward.

- Another key opportunity for Jamf is to expand within the large organizations (5K+ employees) that already use its solution for device management. The added value and broader appeal that the integrated Wandera capabilities will deliver around security for hybrid work environments certainly has the potential to help Jamf expand adoption with this segment. Important to achieving this will be in Jamf furthering its partnerships with the likes of Microsoft and Google that have a strong, established enterprise footprint. Such partnerships will benefit customers by providing a diverse and feature-rich set of capabilities that support efforts to manage and secure multi-OS environments.

Market impact

- Jamf's solution is commonly adopted by global commercial, education, and healthcare organizations that have a large deployment of Apple devices—whether they be macOS, iOS, iPadOS, tvOS, or a blend of all. Jamf currently has strong adoption amongst North American organizations, with a lot of potential to grow its traction amongst European and Asia & Oceania businesses. Jamf supports customers that adopt both BYO and corporate-owned management programs.

- The explosion of interest in remote and hybrid working has seen Jamf experience very strong revenue growth over the last financial year. Jamf advises that business demands around secure remote access, single sign-on, and cloud enterprise applications and workflows are

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

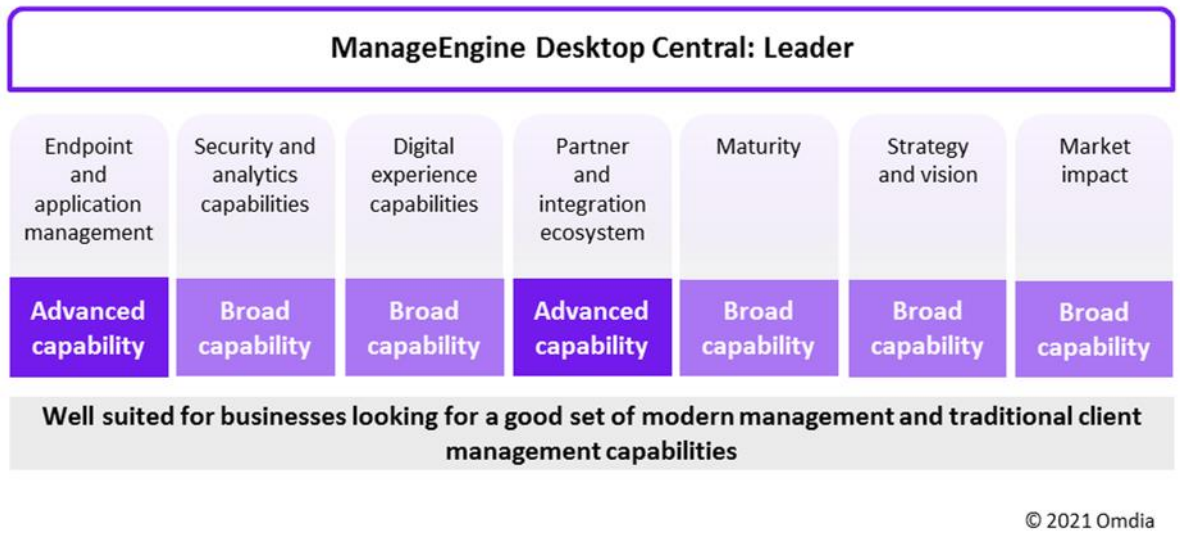
driving a lot of interest. Jamf looks to further increase its market impact by continuing to develop its capabilities into an Apple Enterprise Management platform experience.

- Jamf's routes to market are direct and via its hundreds of global partners that include system integrators, managed service providers, and telco providers. IBM, DXC, DoCoMo, Wipro, Verizon, and T-Mobile are a few examples of the partners Jamf currently works with.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

ManageEngine Desktop Central

Figure 12: Omdia Market Radar recommendation—ManageEngine Desktop Central



Source: Omdia

Why consider ManageEngine Desktop Central?

- ManageEngine has good experience in supporting organizations with solutions that enable mobile and more traditional client management via a single platform and approach. ManageEngine's UEM solution helps organizations manage and secure different endpoints across their entire lifecycle, and the vendor's mobility management capabilities are complemented by the vendor's traditional client management capabilities—something that is important considering how many enterprises are still transitioning to UEM and have portions of their endpoint ecosystems that still need to be managed using traditional CMT workflows.

- Desktop Central supports and offers a single license model that covers a broad range of different endpoints, including Windows (from Win XP to Win 10), Windows Server, macOS, ChromeOS, iOS, Android, Linux, and wearables including Google Glass, Apple Watch, and Microsoft HoloLens. ManageEngine does not add any additional fee for businesses to manage PCs. This enables organizations to take advantage of both modern management and traditional PC lifecycle management capabilities without having to rush any migration process that could be costly.

- As is the case with most UEM vendors, mobile workforce security capabilities are a vital part of ManageEngine's modern management proposition. Desktop Central enables customers to undertake all endpoint security and management activities via a single console and set of

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

workflows. This capability is having an impact on how ManageEngine is looking to position its UEM offering going forward, with the vendor working on making its solution a bridge between IT Ops and Sec Ops teams, helping these teams move away from the many different dashboards and security processes that are common.

Roadmap and areas of future focus

- One of ManageEngine's (and parent company Zoho's) strengths is in the breadth of different enterprise IT products it currently delivers. ManageEngine recognizes the importance and growing need for an integrated set of digital workplace capabilities that help businesses improve endpoint and application management, communication and collaboration, security, workflow automation, and employee productivity. The automated workflow capability delivered via integration between Desktop Central and ManageEngine's IT Service Management is a good example of how the integrated set of capabilities can support broader workplace transformation efforts. ManageEngine will also invest resources in further enhancing Desktop Central's security, employee experience, and automation capabilities in line with business demands for capabilities to support more diverse and mobile work styles.

- Whilst Desktop Central is a solution that integrates well with other ManageEngine- and Zoho-native products, it does not offer the same level of rich integration with popular mobile security solutions offered by some of its peers in the UEM space. For example, the product does not currently integrate with MTD solutions, nor does it offer native capabilities in this area. ManageEngine should look to further develop how Desktop Central integrates with other third-party mobile security and productivity products.

- Growing its SaaS business is another area of focus for ManageEngine. Currently, most Desktop Central customers deploy on-premises UEM, but the vendor is looking to grow adoption of its SaaS offering. ManageEngine advises that it has made good progress since launching its UEM suite on Zoho's own cloud platform in early 2020. The pandemic and shift to remote work has seen many customers prefer an on-demand model, and it is now seeing adoption of its SaaS UEM solution for the same.

Market impact

- ManageEngine has experienced strong adoption of its UEM capabilities over the past twelve months, and the vendor reports strong UEM-related revenue growth over the same period. The US is currently ManageEngine's most successful market, with adoption by European organizations also being strong. Initially, for English-speaking countries, ManageEngine adopted a dual model of both direct and channel-driven business. For other regions, adoption has predominantly been via channel partners. ManageEngine is now rapidly expanding its physical presence across the globe so that vendor becomes better positioned to manage these channel partnerships and strategic enterprise accounts more regionally, rather than managing them all from the US.

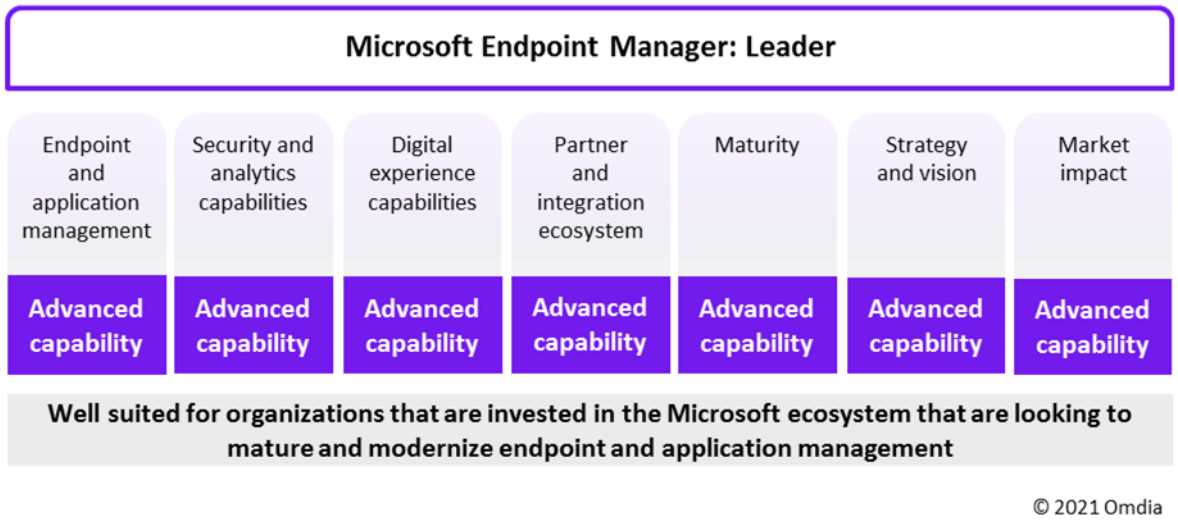
© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

- It is typically mid-size enterprises that adopt Desktop Central. ManageEngine has been making progress in growing adoption in the enterprise market over the past 3–4 years, reporting impressive growth with enterprises managing 10K+ endpoints.
- Key to ManageEngine's GTM approach is in advocating the value of a consolidated suite of products from a single vendor. Beyond UEM, ManageEngine offers solutions across areas such as identity and access management, security information and event management, enterprise service management, endpoint security, and IT operations management and analytics. The company is currently working on a single, unified agent that will bring together this entire ecosystem of products for customers.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Microsoft Endpoint Manager

Figure 13: Omdia Market Radar recommendation—Microsoft Endpoint Manager



Source: Omdia

Why consider Microsoft Endpoint Manager?

- Microsoft Endpoint Manager (MEM) brings together different Microsoft 365 capabilities, most notably Intune and Configuration Manager, in helping organizations manage and secure mobile devices, servers, traditional desktops and laptops, virtual machines, and Microsoft's new Cloud PC offering through a single portal and set of policies. MEM's strong set of UEM capabilities, its rich integration with other Microsoft and third-party products, and the attractive licensing model—especially with so many organizations already invested in the Microsoft ecosystem—has seen the solution differentiate and experience strong adoption and success over recent years.

- As organizations and IT departments continue to be challenged by the speed and scale of employee support activities, including the provision of new devices and applications, capabilities that can help them operate at greater scale whilst delivering a positive service experience will be important. Windows Autopilot is part of the MEM offering and can help with such challenges by enabling organizations to preconfigure devices around different personas and automatically enroll devices in Intune for management and security purposes. The user experience improves as the devices and apps an employee needs will be ready to use and secure on receipt, with no manual intervention required. Microsoft is also simplifying how organizations can deploy applications to managed and unmanaged devices by bringing together the capabilities of the Microsoft Store and Windows Package Manager with MEM. Essentially, this integrated set of capabilities will enable businesses to deploy and

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

manage its catalog of different apps, including Win32, .NET, Universal Windows Platform (UWP), and Progressive Web Apps (PWAs), from within Intune.

- At the core of MEM's value proposition for some time has been its co-management capabilities. One of the biggest barriers to a modern management approach supported by UEM is often the investments and policies that organizations have in legacy and on-premises policy and endpoint management. Co-management enables organizations to migrate at a more comfortable pace by allowing businesses to keep some legacy configuration management tasks and workloads on-premises whilst migrating others to the cloud with Intune. Given the popularity of Microsoft System Center Configuration Manager (SCCM), this phased migration approach is one that the enterprises Omdia engages with very much favor.

Roadmap and areas of future focus

- Modern management capabilities will play a vital role in how the modern workforce is secured and enabled. The mass shift to hybrid work and the ongoing change in the work styles employees are gravitating towards has made MEM very important to Microsoft's overall enterprise strategy. Continuing to expand MEM's capabilities to support organizations managing and securing diverse endpoint and application ecosystems that extend beyond Windows and 365 apps will help Microsoft further elevate the appeal of its solution. Additionally, support for the deployment and management of third-party apps and capabilities to help manage and secure ChromeOS are examples of features that would enhance Microsoft's offering even further.

- Helping organizations better understand, measure, and positively impact the employee experience (EX) has been a focus for Microsoft for some time, and the vendor has further increased its commitment in this area recently, most notably with the introduction of the Viva employee experience (EX) platform. The data, insights, and workflows that MEM helps manage are all important in understanding EX and the impact of technology on people, so the integration between MEM and capabilities such as Viva will be a key strategic focus for Microsoft going forward.

- The release of Windows 11 will intensify interest amongst organizations around device and OS refreshes and cloud-enabled endpoint and application management. This, coupled with the need organizations have in managing and securing a more mobile and hybrid workforce, will further intensify interest in UEM solutions. Microsoft must continue to educate the market on the value of MEM and modern management in combination with the likes of Windows 11 and Windows 365 Cloud PC in helping businesses enable and secure hybrid work.

Market impact

- Microsoft has achieved impressive traction of its modern management capabilities recently, with more than a 250% growth in customers managing their Windows endpoints in the cloud over the last fiscal year. MEM is well adopted by organizations from across all geographies and verticals, including organizations in highly regulated industries.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

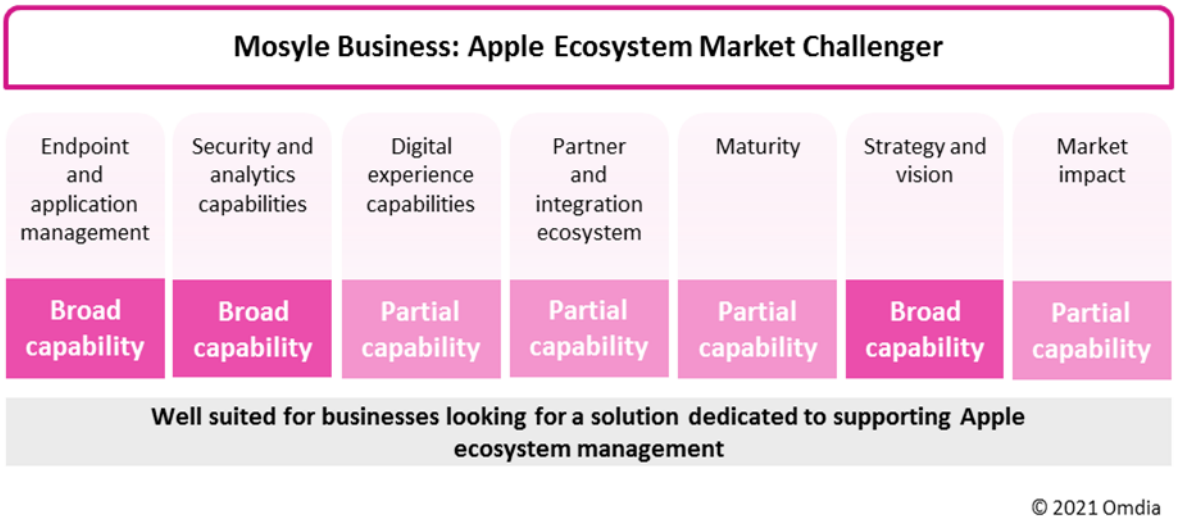
- Microsoft has made clear its intent to better enable frontline workers with its solutions, and endpoint and application management capabilities will have an important role to play here. Frontline worker solutions are impacting the enterprise IT market, with more enterprise technology and business leaders strategizing around how the front and back-office can be better connected to deliver better employee and customer experiences. As frontline workers become more empowered with digital capabilities, being able to easily administer and secure these experiences will be important—something that solutions like MEM can help with.

- In addition to its direct route to market, Microsoft also boasts an impressive partner ecosystem that spans system integrators, IT service providers, and telcos, amongst others. MEM is an important UEM offering and component of the managed mobility and digital workplace services that many partners deliver.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Mosyle Business

Figure 14: Omdia Market Radar recommendation—Mosyle Business



Source: Omdia

Why consider Mosyle Business?

- Mosyle exclusively supports Apple devices and iOS ecosystems. The vendor is a new entrant to the Omdia UEM Market Radar this year. Mosyle's first MDM tool—Mosyle Manager—was launched in April 2016. This was an Apple ecosystem MDM solution developed for the education industry. After achieving strong customer growth in the education sector, the vendor launched Mosyle Business in 2019 as an alternative MDM solution for Apple enterprise customers. With its specialized solution, Mosyle aims to provide a modern, cloud-first approach to Apple MDM at an attractive price point.

- Mosyle places a strong emphasis on customer support by having a dedicated team that works with each customer from the outset to ensure they become competent in the use of its solution, helping businesses get maximum value from adoption. Mosyle's approach is to support organizations invested in the Apple ecosystem with good technical and support capabilities to help reduce the complexities associated with mobility management.

- In addition to an attractive price point for larger deployments, Mosyle also offers a free solution for businesses looking to manage under 30 Apple devices that deliver the same feature set of its premium version.

Roadmap and areas of future focus

- Mosyle will remain focused on building products tailored specifically to the demands of businesses and education customers that are invested in the Apple ecosystem. Mosyle

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

empowers its experienced technical MDM experts to work directly with clients, especially during the sales approach and lifecycle. The company does this to maximize the value customers get from its solution and to be able to more quickly adapt its product based on customer and technical feedback received.

- Compared to some of its peers in the space, Mosyle is a relatively new entrant into an established UEM market. In addition to its attractive price point and specialized Apple ecosystem proposition, Mosyle must continue to develop capabilities that help it differentiate from competitors in this space. Mosyle's customer-centric approach and focus are also very good, but as the organization grows, it may be difficult to scale that same level of support. Mosyle must find a balance between delivering the support customers need and appreciate, but at a level that will not limit the organization's ability to grow and retain good customer sentiment further.

- The Apple ecosystem endpoint management and security market is currently dominated by Jamf, so raising its market awareness will be important if Mosyle is to further increase adoption, especially amongst mid-to-large sized organizations. Mosyle recently made a new leadership appointment to support its growth objective. In September 2021, Mosyle appointed Michael Donlan—a former Microsoft and Apple Executive—as chief operating officer to help guide the company's future strategic direction.

Market impact

- At the time of writing, Mosyle has 23,000+ customers and reports that it manages millions of devices daily. Mosyle is focused on delivering highly specialized capabilities in helping SMEs, enterprises, and education customers. The vendor helps these organizations manage and secure endpoint environments that scale from 30 to 100,000 Apple devices.

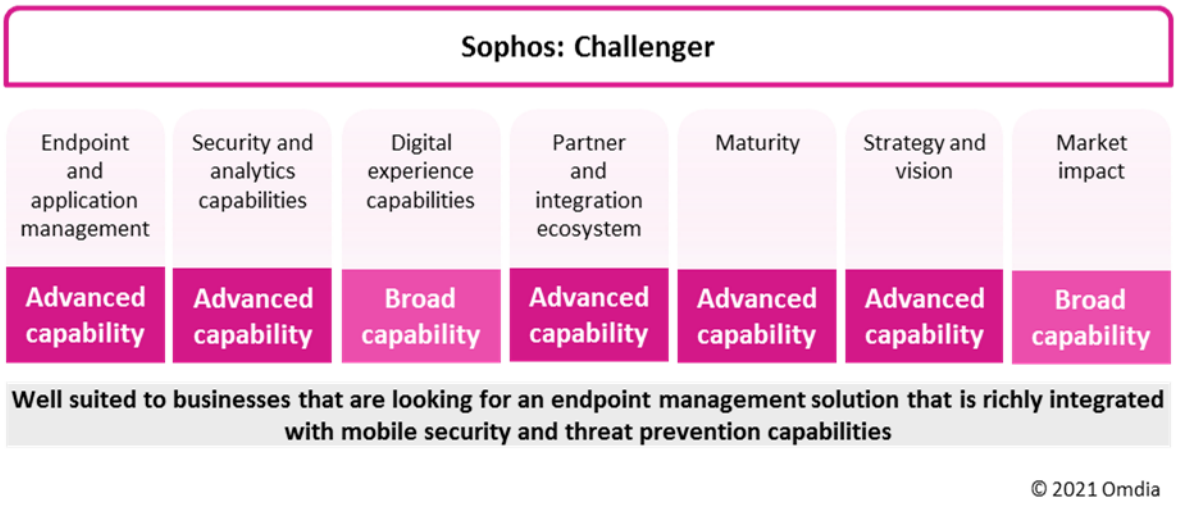
- Mosyle supports businesses with its SaaS-only UEM solution across all industries. It currently has customers in 90 countries across North America, South America, EMEA, Asia, and Australia.

- Mosyle has been subject to significant investment these past few years, with the latest round of funding being in November 2020. This investment of $32m was the most significant Mosyle has received since the company was founded.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Sophos

Figure 15: Omdia Market Radar recommendation—Sophos



Source: Omdia

Why consider Sophos?

- Sophos focuses on tightly integrating endpoint management capabilities with mobile security and threat prevention features that enable customers to manage and secure a workforce that is reliant on a diverse estate of devices and applications. The vendor's UEM capabilities are also tightly integrated as part of its Sophos Central platform. This platform offers customers the UEM capabilities alongside Sophos's enterprise security portfolio of solutions, supporting approaches where organizations are looking to unify mobile security with wider enterprise security practices and approaches. The consolidated application stack and unified management console provided by Sophos Central also deliver a strong set of reporting and analytics capabilities that can be used to improve security and technical support practices.

- Sophos's portfolio of security solutions, including its UEM capabilities, are powered by Sophos Labs and Sophos AI—the vendor's global threat intelligence and data science operations. This technology enables customers to benefit from the same advanced protection across each of the device platforms they manage, including desktops, mobiles, or servers. In addition to the technical capabilities, Sophos also has its own threat investigation and research team and is an active Cyber Threat Alliance member.

- Improving technical support at scale has become an important objective for organizations, especially since the switch to more hybrid and mobile work styles. Sophos offers capabilities that can help support teams to improve the digital experience for employees. Sophos Live

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Response enables admins to undertake system-level remote control of devices, improving the way they can support and troubleshoot issues across devices. Additionally, integration with TeamViewer facilitates remote support through device screen sharing and remote control.

Roadmap and areas of future focus

- Further investing and developing its platform that helps businesses strengthen enterprise security is key to Sophos's roadmap. Sophos observes that organizations are increasingly not viewing device management and device security as being separate entities: businesses increasingly want to manage and protect devices side-by-side, irrespective of whether they are mobiles or desktops. The consolidation of endpoint management and security capabilities has therefore become an important product strategy for Sophos.

- In addition to enhancing its own native products, including UEM, Sophos is also focused on making the integration process easier. Sophos is increasingly focused on an "API first" model, meaning new features are designed around being available through public APIs, enabling customers to easily integrate Sophos's features and services into their own systems.

- Sophos's UEM capabilities are currently well adopted by small and mid-sized organizations, but traction of Sophos's UEM solutions amongst larger enterprises is smaller when compared to some of its peers in this space. Growing adoption amongst the enterprise segment is achievable as Sophos's UEM capabilities and security focus would have appeal amongst larger organizations, especially those that may already use another Sophos solution.

Market impact

- Sophos goes to market entirely via its channel partners. Sophos currently has over 71,000 channel partners, spanning system integrators, IT service providers, and telcos. This partner ecosystem is supported by Sophos's dedicated global enablement and certification team that delivers an extensive program of ongoing partner certification and training activities. For new technology and product introductions, new certification classes and training modules are introduced throughout the global partner base through a combination of in-person classroom training and remote learning.

- Sophos operates across all major geographies and industries, with the EMEA region being the vendor's strongest in terms of adoption. In some regions, Sophos has industry-specific teams that work exclusively with customers and partners in that field (in healthcare, for example).

- Sophos has experienced strong revenue growth this past financial year, driven by the increased priority organizations are placing on mobile security and management solutions. Whilst Sophos's market share and recognition are not as great as some of its UEM peers, its strong set of capabilities and its strategic commitment to enterprise security certainly have

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

the potential to help the vendor increase its UEM market impact, especially amongst security-conscious mid-to-large sized organizations.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

VMware Workspace ONE

Figure 16: Omdia Market Radar recommendation—VMware Workspace ONE

Source: Omdia

Why consider VMware Workspace ONE?

- One of VMware's key strengths and differentiators is the comprehensiveness of its solution. In addition to the management and security of a diverse range of different endpoints, including desktops, mobile, rugged and IoT devices, and thin clients, Workspace ONE is also a comprehensive analytics and automation platform. Workspace ONE also includes full desktop lifecycle management capabilities.

- With its Digital Employee Experience Management (DEEM) capabilities, VMware can help organizations better measure and improve the employee experience, specifically relating to how people use and feel about the digital tools they rely on for work. DEEM aggregates device, user, app, and OS data in developing a baseline score and view of what the employee experience looks like. Actionable insights based on this data can then be leveraged to help improve employee experiences. DEEM also enables businesses to automate important IT support troubleshooting and remediation processes. More sentiment-based features, including contextualized employee surveys and methods for real-time employed feedback, further strengthen the insights DEEM delivers, as do the network intelligence capabilities that are soon to be introduced into the solution.

- In embracing more hybrid and mobile-first work styles, businesses must not only consider how a diverse app and endpoint ecosystem must be managed and secured, but also how the workflows and processes that guide the tasks and work people undertake must also evolve and be digitized. Workflow development and automation platforms are becoming important

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

in supporting this need. Freestyle Orchestrator is VMware's workflow and IT orchestration solution that allows admins to develop digital workflows that can be automated via a drag-and-drop interface.

Roadmap and areas of future focus

- In April 2021, VMware launched Anywhere Workspace—a solution that combines different VMware capabilities—including Workspace ONE and VMware Horizon, VMware Carbon Black, and VMware SASE, amongst others—in one proposition. The introduction of Anywhere Workspace represents an important strategic step for VMware, one that will see the vendor look to further establish itself as an important workplace transformation partner. VMware has introduced Anywhere Workspace to help businesses support a modern workforce that is device-agnostic, secure, and empowered to work productively from any location. The combined and integrated capabilities offered by VMware's Anywhere Workspace solution will be attractive to organizations looking to improve employee productivity, standardize and simplify technology ecosystems, and help businesses improve workplace security and management practices.

- VMware's all-in-one and native mobile and client management capabilities are certainly well-suited to organizations looking to embark on a big-bang transformation approach to modern endpoint management. However, co-management capabilities do have value for organizations that do not wish to make a big bang approach and transition away from more traditional and often well-engrained client management capabilities.

- VMware currently develops solutions suited to the needs of different verticals, but its vertical focus and strategy continues to mature. VMware recently formed a new industry solution and customer transformation team to further drive traction and the value realized by organizations across the key verticals of government, healthcare, financial services, retail, manufacturing, and telecoms.

Market impact

- Workspace ONE is one of the most widely adopted and recognized UEM solutions available on the market. VMware's GTM strategy for Workspace ONE is multichannel, multi-route, and global. EUC has dedicated sales teams covering named accounts across the enterprise and larger commercial segments. The solution has strong traction amongst large enterprise customers and can be deployed as SaaS or on-premises.

- VMware works with 30,000+ partners worldwide, and the vendor has strong relationships with global telcos. These telcos—including AT&T, Verizon, Sprint, NTT Docomo, Rogers, Deutsche Telecom, Vodafone, Telefónica, and Orange—leverage Workspace ONE as an add-on capability with commercial and enterprise data plans and device sales. VMware also works with systems integrators and outsourcers, including DXC, IBM/Kyndrel, Deloitte, Accenture, HP, Wipro, and Cognizant. These partners support customers worldwide on the strategic adoption and ongoing use of VMware's capabilities.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

- VMware has a history of acquisitions that have significantly strengthened its overall value EUC value proposition. Recently, VMware has made additional acquisitions that further strengthen its market impact and solution, including that of SaltStack (event-driven automation for IT and SecOps), Nyansa (network intelligence and analytics), and LastLine (threat detection)—all of which will further strengthen VMware's end-user computing proposition.

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.

Appendix

Methodology

This report utilizes responses to a comprehensive Omdia capability matrix, in addition to briefings. This was accompanied by insights gathered via TrustRadius and secondary research and data from sources, including Omdia's 2021 *Future of Work* survey.

Author

Adam Holtby, Principal Analyst, Digital Workplace

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com

© 2021 Omdia.
All rights reserved. Unauthorized reproduction prohibited.