

The Business Value of Unified Endpoint Management

A Comparison of Market Leaders

By Eric Klein, Director, with David Krebs, Executive Vice President

Table of Contents

Introduction

Methodology

Endpoint Management Market Definition

“Old Guard” vs. “Mobile First”

Exhibit 1: Endpoint Expansion Beyond the PC

The Changing Endpoint Management Landscape

Exhibit 2: The New Endpoint Management Landscape

Seamless Integration Driving Next-Gen Endpoint Market Opportunity

Exhibit 3: Desirability of Potential Future Endpoint Management Capabilities

Changing Work Patterns Forcing Organizational Change

Mobile Influx Changes Endpoint Management Paradigm

Exhibit 4: Supporting Mobile Deployments Comes with Many Challenges (percent of respondents; n=90)

Competitive Landscape

Sentient Endpoint Manager (previously known as Radia)

Challenges Facing the Mobile-First Vendors' Pivot

Exhibit 5: Accelerite Sentient Endpoint Manager SWOT Analysis

IBM Endpoint Manager (Version: 9.2)

Exhibit 6: IBM Endpoint Manager SWOT Analysis

Microsoft System Configuration Manager (Version: SCCM 2012 RC2)

Exhibit 7: Microsoft System Configuration Manager SWOT Analysis

Exhibit 8: User Ratings: Security, Reliability/Uptime, Platform Support Options, and Costs

Administration Requirements:

Exhibit 9: Factors that Affect Scalability

Conclusion

Background on Accelerite

Appendix A: Baseline Organization Description

Disclosures

Disclaimer

VDC Research

About the Author

About VDC Research

Introduction

As the line between personal computers and mobile devices continues to blur, and the number of non-traditional endpoints that need to be managed expands, implementing an endpoint management solution with the right architecture and governance model will be increasingly important for IT organizations. Diversity in endpoints, along with the influx of mobile devices in the enterprise, has created significant challenges for IT from a management, security, and support perspective. In recognition of this pain point, market leading endpoint management vendors have spotted an opportunity to manage these endpoints with their enterprise-grade solutions. These vendors have quickly moved to incorporate robust mobile device management (MDM) functionality into their products and have optimized their platforms to protect an increasingly diverse range of non-traditional endpoints (e.g., ATMs, kiosks, smart vending machines, parking meters, POS devices etc.) along with the mobile device(s) that many of us are carrying into the workplace. The increasing reliance on connected endpoints and cloud-based applications has made offering secure and predictable IT services to customers, business partners, employees on a 24x7 basis a requirement in the business world and has made IT infrastructure investments for next-generation endpoint management a priority for CIOs, CISOs, and IT leaders. Next-generation solutions must not only be endpoint agnostic but must be able to compile data from all potential sources across network elements, data on email and web gateways, mobile devices, software and applications, virtual environments, and the cloud to gain knowledge about their endpoint environment, identify potential threats, and enable the ability to enforce consistency in policies. They should also be tightly integrated with agile systems that cover the network, mobile devices, and the cloud. These solutions need to be extensible, built for scale, and centrally managed for unified policy and consistent controls. Vendors are moving quickly to federate these capabilities via a unified administrative console that not only simplifies endpoint management processes, but ensures that their solutions are non-intrusive to the end user experience while delivering an opportunity to break down the silos created by the wide variety of point tools that exist in the market today. This white paper will focus on market-leading endpoint management solutions that are available in the market today. This report compares and contrasts several of the key capabilities that exist within three popular endpoint management solutions (Accelerite's Sentient Endpoint Manager, IBM's Endpoint Manger, and Microsoft's System Center Configuration Manager – SCCM). It also provides an independent view of the strengths and weaknesses of each of these products for unified endpoint management and will help senior IT, business decision-makers, and key influencers within these organizations navigate the complexity of implementing and evolving their endpoint management strategy.

Methodology

VDC Research surveyed more than 90 IT decision-makers who either had direct involvement in the purchase of and/or usage of the endpoint management solutions in use at their organization. We also researched IT perspectives relating to endpoint management and conducted in-depth phone interviews with end users of the three vendors (Accelerite, IBM, and Microsoft) evaluated in this white paper.

Hardware, software, and cost information was provided by study participants; in some cases, list pricing was used in lieu of actual pricing to reduce the impact of vendor discounts from the analyses or when actual purchase prices were not available.

Endpoint Management Market Definition

Endpoint management solutions have long been relied on by IT organizations to manage their PC and server deployments. These solutions typically utilize a policy-based approach to endpoint management and enable IT administrators to ensure that the devices they are managing are protected and fully compliant with the policies they have implemented. Endpoint management solutions have proven to be invaluable in large deployment environments and feature powerful capabilities to automate system administration and support functions that would otherwise need to be performed manually. IT organizations have become reliant in these solutions to provision applications and configuration changes (software updates and patches), for asset management, remote management and troubleshooting, vulnerability and compliance management, remediation of endpoints that go out of compliance, as well as enforcing configuration policies. The inventory and asset management elements of these solutions are also extremely important and enable organizations to quickly access their software assets for license reconciliation or compliance purposes.

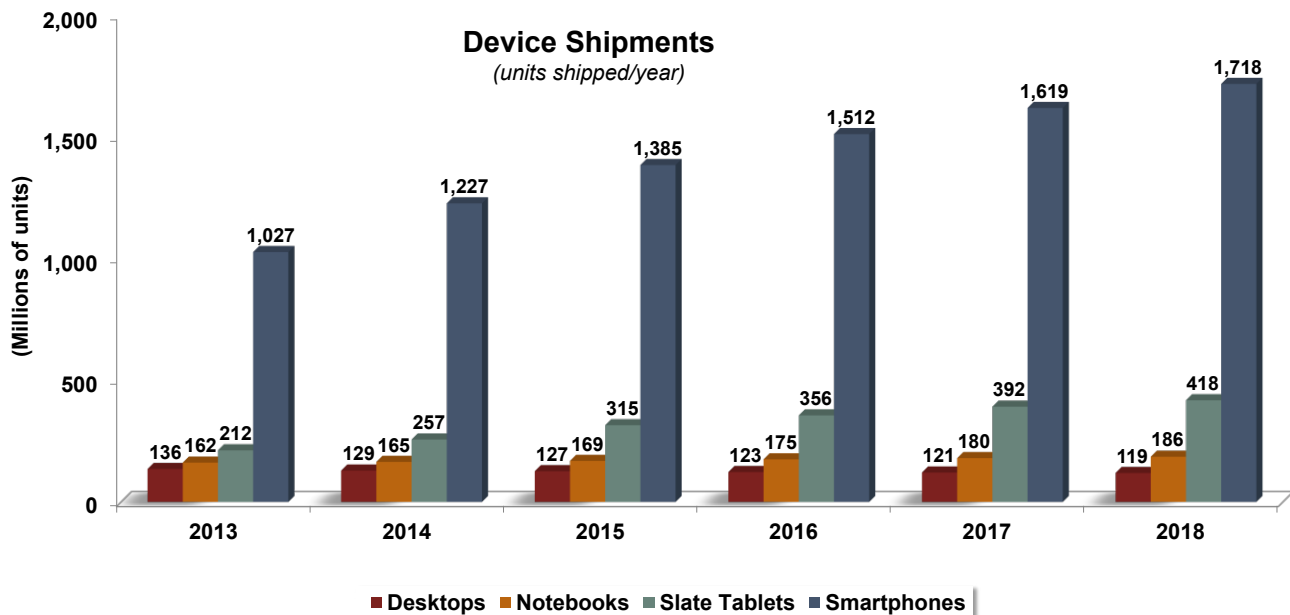
Vendors are actively engaged in developing next-generation endpoint management solutions; however, the market is varied and in a state of flux, as enterprise needs are varied and a holistic “one size fits all” solution remains elusive. To date, the majority of the devices being managed by endpoint management solutions has been desktop PCs and servers; however, the rapid expansion of mobile devices and non-traditional endpoints (e.g., ATMs, kiosks, smart vending machines, parking meters, etc.) has necessitated that endpoint management solutions evolve; enter Unified Endpoint Management. These solutions’ objective is the full lifecycle management of endpoints regardless of form factor or operating system (OS). These solutions offer the potential for an organization to utilize a single vendor and systems management platform to support their increasingly diverse deployment environments.

“Old Guard” vs. “Mobile First”

The continued influx of mobile devices into the workplace has quickly made extending endpoint management to popular mobile platforms from the likes of Apple, Google, and Microsoft a requirement for IT organizations. Traditional endpoint management vendors (“the old guard”) have a rich history of delivering proven enterprise-grade solutions to manage corporate productivity devices that provide employees access to critical business systems while retaining usability and ease of management for administrators, however; they have only recently augmented their solutions with mobility management functionality. These vendors now recognize that providing end-to-end support that enables administrators to inventory, deploy, patch, and continuously manage both PCs and “modern endpoints” across heterogeneous hardware is required; however, their challenge will be to demonstrate that they can match the level of innovation and functionality of new “mobile-first” entrants into the market and offer a modern user experience for managing non-traditional endpoints.

Traditional endpoint management vendors added mobility management capabilities to their platforms out of necessity as they continue to see explosive growth of non-traditional endpoints in their customers’ deployment environments. Exhibit 1 shows VDC’s device shipment estimates through 2018; managing mobile devices is without question a requirement moving forward for all enterprises.

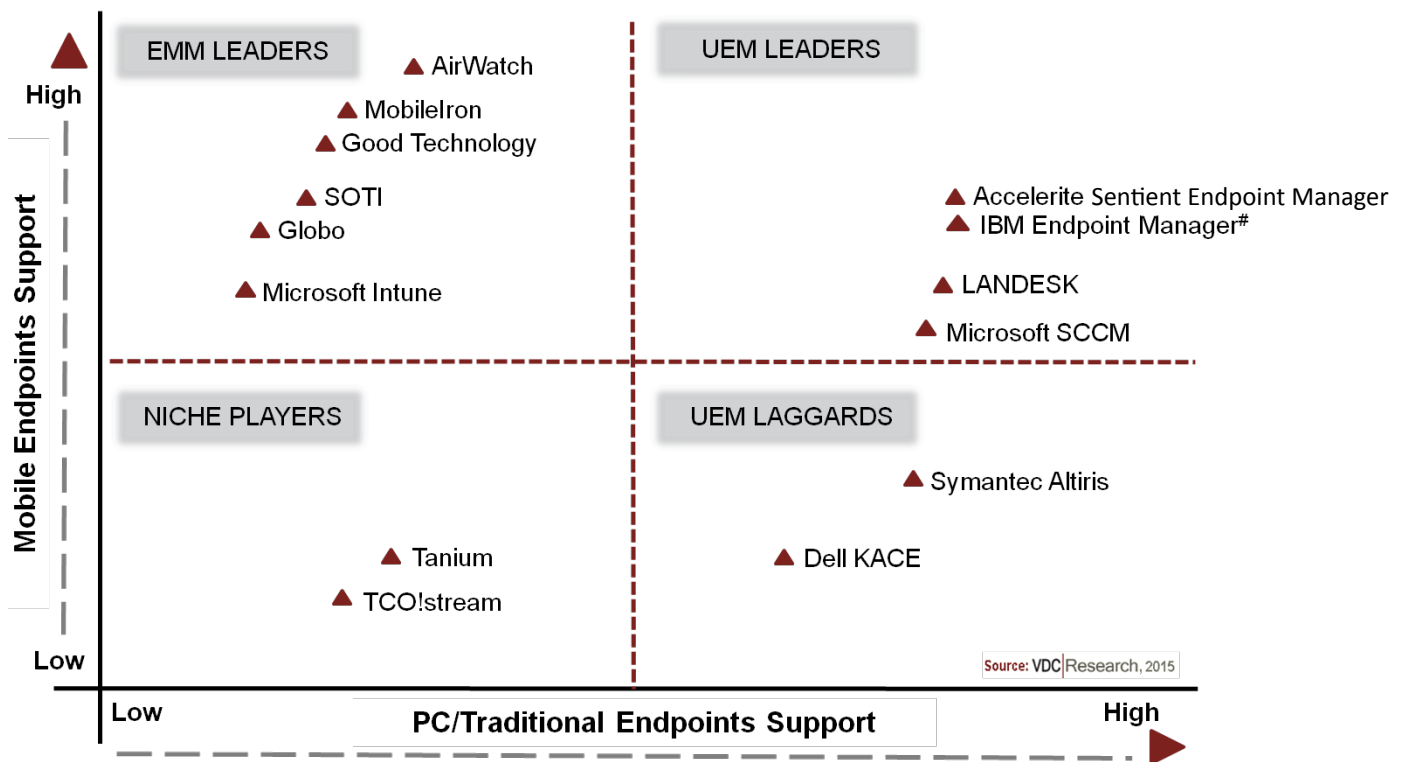
Exhibit 1: Endpoint Expansion Beyond the PC



The Changing Endpoint Management Landscape

The following chart indicates key players along traditional/PC management space (horizontal axis) and mobility endpoint management space (vertical axis). EMM players (top-left quadrant) specialize in mobility management almost exclusively, while traditional or PC management players (bottom-right quadrant) specialize in managing PCs, servers, and virtual environments. The bottom left quadrant contains players that are operating in a niche or are upstarts that are trying to disrupt using newer delivery models such as Cloud, or are adding complementary capabilities such as analytics, endpoint monitoring, etc. Very few players are implementing mobility management as well as PC management, and thus operating in the top-right Unified Endpoint Management quadrant.

Exhibit 2: The New Endpoint Management Landscape



*Relative positions are only indicative and not set to precise scale.
 #Success and quality of MaaS360 product integration will improve IBM's mobility support

This model of evaluation is critical for IT departments to internalize because unified management of PCs and mobile devices can potentially provide them with operational and cost efficiencies that can go far beyond what they can get from separate point tools, in addition to the savings realized on licensing costs of the tools themselves. The efficiencies come from shared use of hardware and policy infrastructure, pooled resources and people, and spreading of other operational overheads across a larger endpoint management base. As a result, these efficiencies provide existing IT administrators with improved organization-wide mobility as well as a broadened career path that currently includes PCs, mobile devices, and future hybrid devices that include the growing segment for IoT based devices and wearables.

The model also includes boundaries (dashed lines separating the four quadrants), which act as key inflection points for the vendors. Crossing each boundary presents a significant strategic and execution challenge for each vendor. While Microsoft, IBM, Landesk, and Accellerite from the traditional PC management side have been able to cross over vertically into the mobile endpoint management quadrant, EMM players have not been effective in crossing over to the right by supporting PCs (with the exception of FiberLink being acquired by IBM and the latter trying to integrate MaaS360 into its existing BigFix architecture). Players like AirWatch and MobileIron have tried adding PC management capabilities, but this has proven to be a daunting task due to the unique nature of the PC ecosystem. Successful management requires supporting a broad spectrum of OS versions that contain legacy platforms, the ability to manage specific operational and technical issues related to scale, performance, and support, and its integration with other essential tools within the enterprise IT system that continue to independently evolve. The difficulty is then compounded by the need to develop these capabilities quickly and thoroughly enough to compete effectively with traditional vendors who have existed and specialized in this market for decades.

On the other hand, in order to be successful, UEM players need to unlock the potential of modern mobile platforms. The key will be to take an approach that can benefit knowledge workers across an entire organization. Our research indicates that IT heads want mobility solutions that will easily and seamlessly integrate with their existing infrastructure investments and their applications. However, given the device diversity that is common in most organizations, there is a need to implement solutions with the flexibility to streamline the management of all devices ranging from the ruggedized device deployments that are common in distribution centers, warehouses, and factories to consumer-grade devices that are finding their way into every business. Additionally, solutions should be able to protect an increasingly diverse range of non-traditional endpoints (e.g., ATMs, kiosks, smart vending machines, parking meters, POS devices etc.) along with the mobile device(s) that many of us are carrying into the workplace. The traditional/PC management players are in a good position to add mobility capabilities and complete their unified endpoint management offering, as is evident with some of them already successfully breaching the boundary to move into the top-right quadrant.

Seamless Integration Driving Next-Gen Endpoint Market Opportunity

Technology advances are enabling businesses to seamlessly extend their applications and workflows to mobile platforms with the transformative potential of mobile, social, cloud, and big data becoming more apparent. The post-PC era is upon us as the opportunity for end users to interact with mobile devices in a business context continues to grow in sophistication. As the lines between personal and mobile computing will continue to blur and the number of “non-Windows” endpoints continues to expand, reinventing your business around what these new platforms make possible will become a critical business priority. The influx of new devices will require IT departments to reconsider how they deliver critical IT services to their internal end users; however, VDC does not recommend abandoning endpoint management tools due to this shift. PCs aren’t going away and will remain as the most prominent productivity platform in the enterprise for years to come – this is due to the application

investments that have been made on PC platforms as well as the business-critical nature of these applications. Exhibit 3 shows that organizations are very keen on acquiring endpoint management solutions that offer seamless integration with their existing infrastructure, visibility across all types of endpoints, and managing of PCs from the same console as mobile devices. VDC urges that organizations give as much importance to these “unifying” considerations as they do to “point” considerations such as acquiring mobility management capability itself or migrating to cloud-based endpoint management.

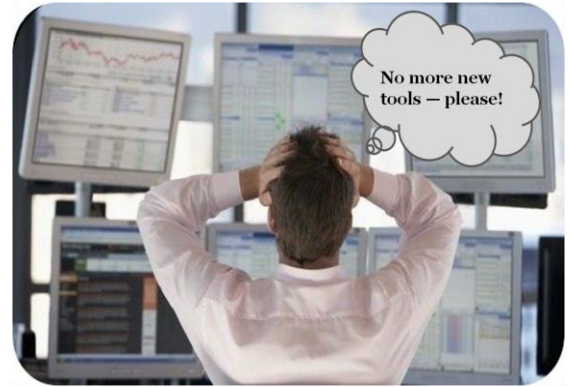
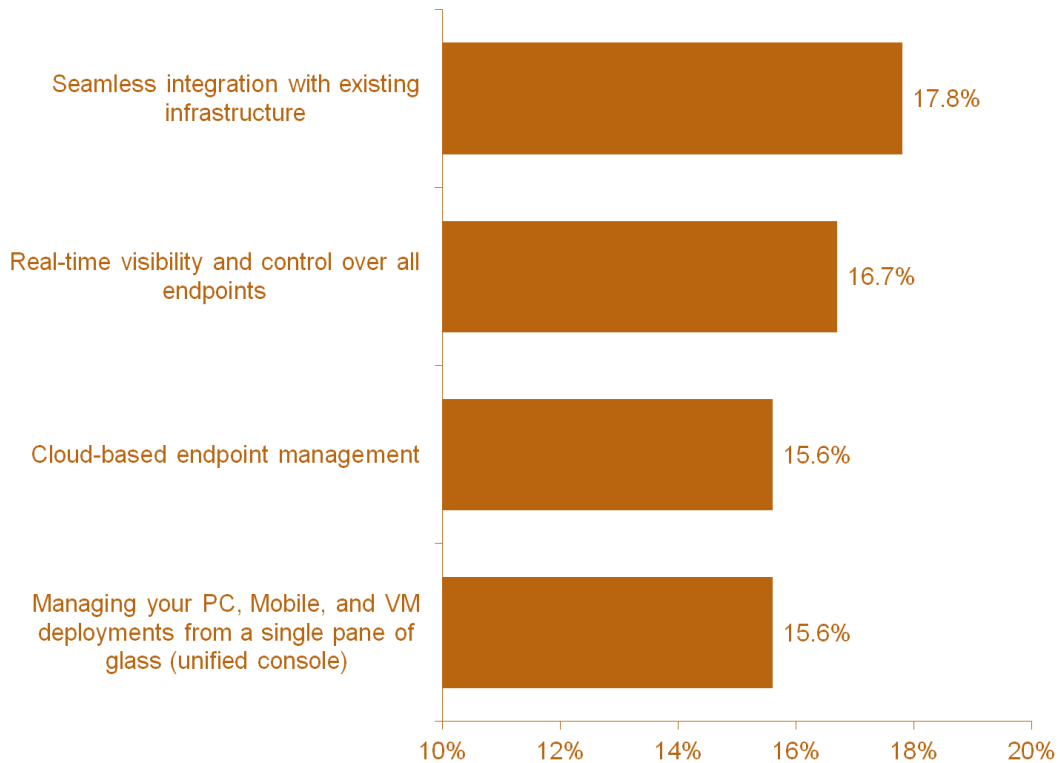


Exhibit 3: Desirability of Potential Future Endpoint Management Capabilities



Changing Work Patterns Forcing Organizational Change

Delivering a consistent end user experience on multiple platforms is perennial challenge from both a technology and an organizational perspective. While organizations are aware of the need to embrace a more user-centric model of computing, users continue to push for access to business applications and content on their own devices and from any location. This is proving to be a challenge for most IT organizations that have yet to determine how to efficiently manage an increasingly broad range of devices. This has created the need to offer robust self-service capabilities to ensure that adequate support is available as well as ensuring that users receive a consistent, secure user experience. Using a personal device shouldn't change a person's ability to access corporate resources, but, at the same time, IT must protect the security of corporate applications and data.

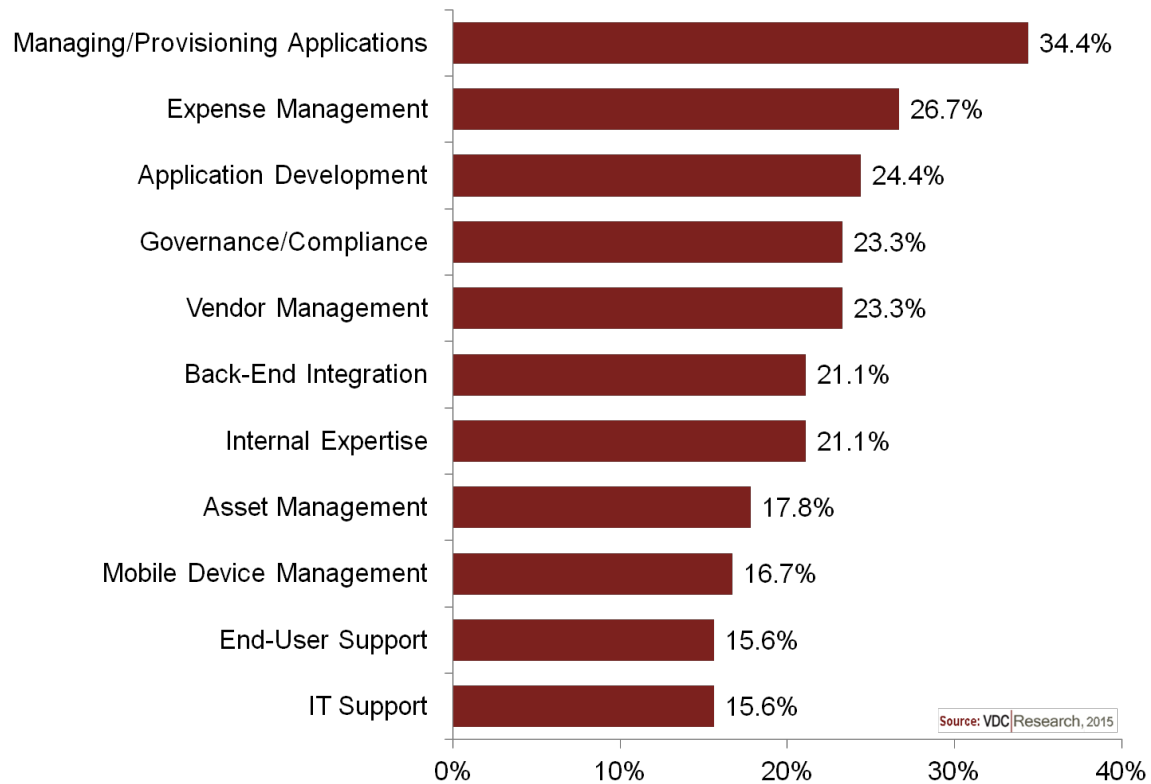
Mobile Influx Changes Endpoint Management Paradigm

The endpoint management landscape is in a state of constant change and has challenged IT with continually assessing how to best secure and manage a multitude of mobile devices on increasingly diverse platforms. Work styles have changed; employees want or need to work at any time or any location, with data that's accessible from the company network, the Web, or the cloud. Given these parameters, IT departments work with a moving target that requires a broad range of measures including user enrollment, application distribution, device configuration, and data security. These requirements in turn impact the organization's enterprise and deployment architectures. Due to the multilayered nature of mobile platforms, security, compliance or management cannot be achieved by finding one ideal hardware configuration or relying on one type of communications network, etc. In a dynamic market, operating systems, applications, devices, and networks are all impacting the endpoint management landscape.

The influx of mobile devices into the enterprise is creating significant challenges for IT from a management and support perspective, particularly once organizations expand their mobile application range beyond de facto horizontal mobile applications like email, messaging, and calendars. Mobile enablement has and will continue to have a profound impact in the enterprise, with the most visible area being the need to invest in solutions to manage and support mobile deployments. Device management remains a cornerstone of security policy for corporate-liable devices. The ability to detect rooting or jail breaking of the operating system, remote lockdown and wiping of the device data, hardware feature controls, and remote control of the device will remain as key features that are requisite to properly protect mobile assets and limit risk in case the device is lost or stolen. However, organizations have come to recognize that they need more, and have been scrambling to ensure their devices are secure. They have turned to enterprise mobility management (EMM) solutions in order to achieve the peace of mind they require to expand mobile deployments and enable access to their corporate applications and content. Mobile enablement will be critical moving forward as pressure continues to mount on employees to work faster and more efficiently. The ability to empower a workforce with true mobile enablement can lead to more informed decision making and even enable an organization to deliver superior customer service. The opportunity

for operational efficiency gains through mobile enablement will become more pronounced, as VDC anticipates that enterprises will continue to integrate mobile applications into their workforce. Exhibit 4 depicts the variety of challenges that organizations face once they begin supporting a mobile workforce.

Exhibit 4: Supporting Mobile Deployments Comes with Many Challenges
(percent of respondents; n=90)



While business leaders are increasingly aware of the opportunity brought by expanding access to critical business applications to mobile platforms, conforming to compliance requirements remains a high hurdle for organizations; particularly those that are embracing BYOD and giving their mobile workforce access to corporate networks, databases, and applications. Moving forward, digital data regulations in industry sectors, such as health care and government, will continue to evolve and will require that companies know exactly where their data is being stored, who is transferring it, and what the level of encryption is for all of their content. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires strict security requirements for protecting electronic protected health information (ePHI); unauthorized disclosure of ePHI is a big risk when using mobile devices because they are small, portable, highly visible, unlikely to be password protected, unlikely to have encrypted PHI, and likely to connect with Wi-Fi (further risking interception).

Challenges Facing the Mobile-First Vendors' Pivot

Enterprise mobility management (EMM) vendors have developed robust solutions to manage heterogeneous mobile platforms and are one of the most visible and competitive market segments in the mobile ecosystem. However, competition among these vendors is fierce, and downward pricing pressure is common due to the entrance of large and established vendors as well as the relatively single-point focus of their solutions. Awareness of the need to evolve their platforms while maintaining visibility in the market has led several prominent EMM vendors to extend their platforms to incorporate PC management capabilities. While several vendors have demonstrated they can grow their roster of large customers, VDC sees challenges ahead to keep pace with the changing requirements in larger deployment environments, where mobility has become strategic to the business. While there are only a small number of enterprises that we would describe this way today, we expect many larger organizations to ingrain mobile solutions into their workflows and business processes. As businesses implement best practices for mobile architecture, user experience, security policies, and standards, they will quickly discover that this will require more advanced and integrated solutions from their technology partners. This trend will potentially have a detrimental impact on mobile-first EMM vendors and will put pressure on these vendors to expand their solution range more quickly and accelerate their pace of innovation.

EMM vendors have found themselves in a strong position and are a significant force in the mobile software market. However, while their solutions are increasingly required as part of a mobile strategy, competition from traditional endpoint management vendors will continue to increase as these vendors have strong brand recognition and broad enterprise portfolios. Years of IT experience and comfort with the current IT domain are crucial for acceptance of any solution, and traditional endpoint management solutions have a definitive edge there over the EMM solutions. Moreover, their ability to add EMM features and incorporate into their fold seems easier to achieve than the other way round.

Competitive Landscape

The market for endpoint management solutions is very fragmented, with mobile device proliferation forcing rapid change in capabilities of the market leading vendors. VDC is profiling the following vendors due to their footprint in the market and their pursuit of a unified endpoint management platform (as evidenced in the Endpoint Management Landscape chart shown above) that includes modern mobile devices such as Apple's iOS, Google's Android, and Microsoft's Windows Phone OS releases.

Accelerite Sentient Endpoint Manager

Accelerite's parent company (Persistent Systems) has acquired exclusive licensing to the former HP client. Automation platform (also known as Sentient Client Automation). Accelerite has rebranded the former HP endpoint management solution as Sentient Endpoint Manager. The Sentient Endpoint Manager platform is comprised of a suite of enterprise-grade and complementary endpoint management products, which are based on a policy-driven architecture that enables IT administrators the ability to manage complex, distributed, and dynamic IT deployment environments. The solution also provides vulnerability and compliance management against industry standards, and security tools

management, which add to its desired state management capability. The company has been actively augmenting the platform and has recently integrated MDM, MAM and EMM capabilities and is expanding its cloud deployment options.

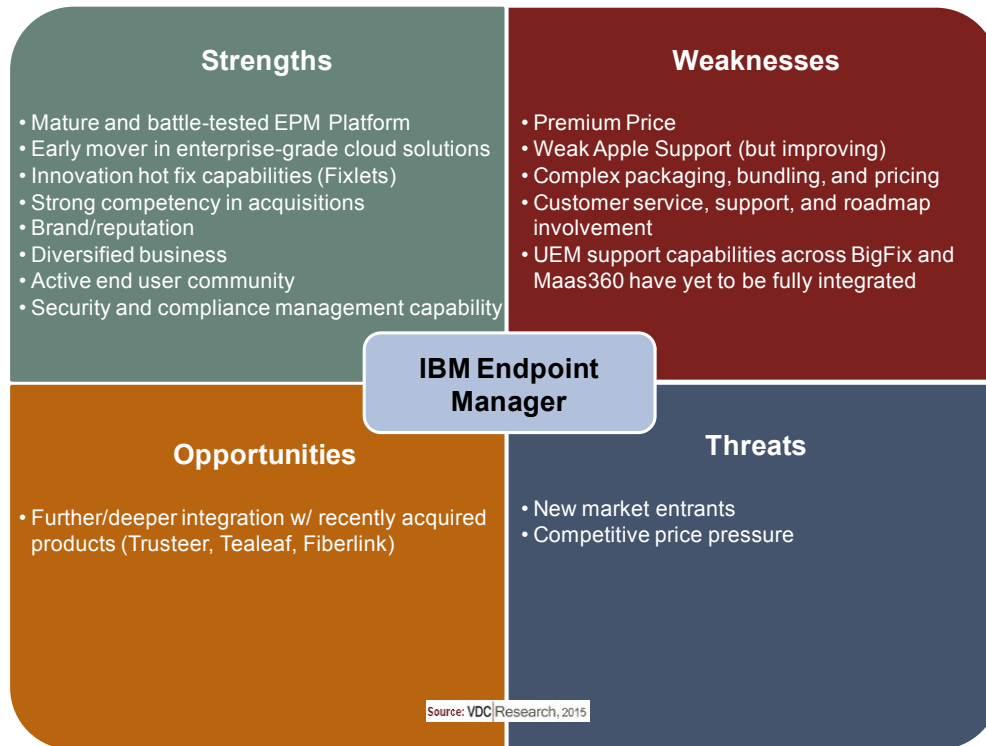
Exhibit 5: Accelerite Sentient Endpoint Manager SWOT Analysis



IBM Endpoint Manager (Version: 9.2)

IBM's Endpoint Manager delivers a unified platform for system's lifecycle and security management of enterprise devices, including data center servers, laptops, desktops, and mobile devices. The solution is based on technology it acquired from BigFix which had developed a comprehensive endpoint lifecycle and security management platform that features an extensible infrastructure to accommodate mobile deployments. This solution enables organizations to proactively manage their servers, desktops, and laptops. Endpoint Manager provides a clear path for improving control and compliance with clear, accurate reporting, and easy integration with systems such as ticketing and change management databases. The company has recently replaced its legacy mobility management solution with the MaaS360 mobility management solution that it acquired via its acquisition of Fiberlink in 2013.

Exhibit 6: IBM Endpoint Manager SWOT Analysis



Microsoft System Center Configuration Manager (Version: SCCM 2012 RC2)

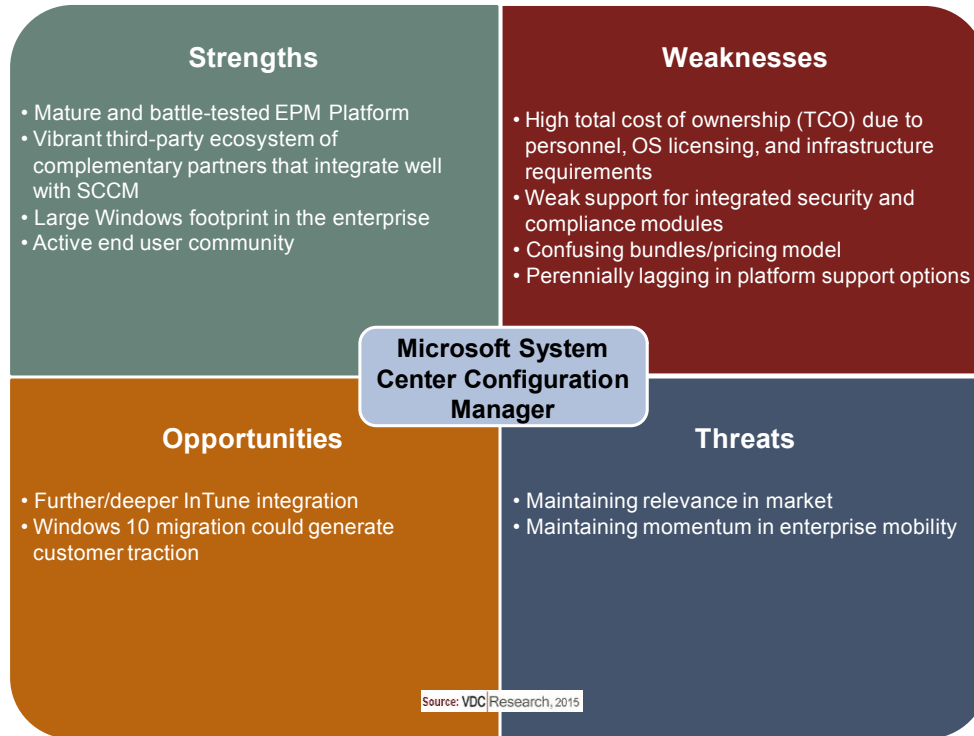
SCCM is Microsoft's enterprise-grade systems management software. The platform can be used to deploy and manage operating systems, applications, software updates, and Microsoft System Center Endpoint Protection (SCEP) policies. The company has recently augmented the MDM capabilities of its cloud-based PC management service (Windows Intune) and has integrated Intune with its SCCM platform. The integration gives Microsoft the ability to offer their SCCM customers a unified platform to monitor and manage their IT environments (including virtual machines and cross-platform mobile devices).

Microsoft's Client Access License (CAL) is a blanket end-user license agreement that is purchased on a per-server/per end-user basis. It is separate from desktop licensing for the Windows OS, the company's Office Suite, or other Microsoft software products.

Microsoft's product diversity should be taken into account particularly as they impact the costs associated with the SCCM platform. Microsoft issues software fixes on a monthly schedule with emergency updates announced frequently outside that schedule; all related endpoints (i.e., desktops, web servers, file servers, communication servers, and data base servers) should be patched along with the systems hosting the security products themselves. This lends additional cost to the overall system maintenance task as well as introduces security

issues because the security products are exposed to the same types of attacks that they are deployed to protect against.

Exhibit 7: Microsoft System Center Configuration Manager SWOT Analysis

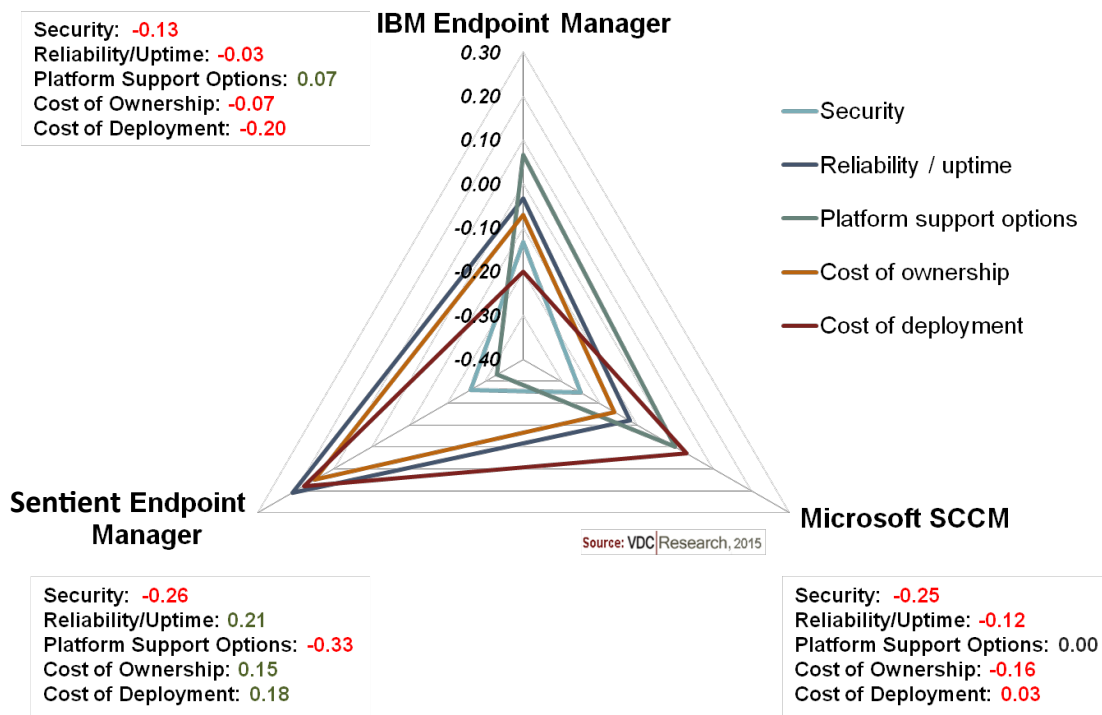


In order to help automate and optimize their IT operations, organizations need modern tools that will help to align IT projects with corporate objectives. Standardizing on a single platform that provides an integrated and company-wide solution that features granular policy control capabilities not only makes sense, but has real potential to reduce costs while mitigating risks. According to recent VDC data, organizations who have invested in an endpoint management solution ranked security, reliability/uptime, platform support options, and cost of ownership and deployment as the most important capabilities of their investments.

There is definitely variance in the licensing fees between the competitive products we've evaluated. However, the largest driver of the difference in total cost of ownership for endpoint management products is professional services and contractors. Through customer and service provider interviews, we learned that over a 5-year period, IBM, and Microsoft customers spend an average of approximately 20% more on configuration and integration services than Accelerite customers. The second-largest differentiator is the cost savings opportunity that comes with efficient administration of applying patches and upgrades. Customers and systems integrators tell us that, on average, non-Accelerite customers spend nearly twice as much on patches, bug fixes, and upgrades as do Accelerite customers over a 5-year period. During our interviews, customers told us Accelerite's tools for applying patches, bug fixes, and upgrades, substantially reduced their overall administration time. However, we found that most survey respondents did not indicate a substantially reduced staff to operate Accelerite's Endpoint

Management products, but that Accelerite required fewer administrators per endpoint. This is in contrast to both IBM's and Microsoft's endpoint management products, which typically require additional administrators to update configuration details as managed deployment environments change and expand. VDC data showed that 16.5% of customers expected the number of endpoints they manage to expand in the next 12 months – Accelerite customers expected the highest expansion rate (17.3%). Additionally, existing Accelerite customers were the most likely to recommend the company's endpoint management solution to colleagues, followed by IBM customers and Microsoft customers. In Exhibit 8, VDC compares the ratings of the three market leading UEM solutions for large enterprise deployment environments (>10,000 employee firms).

Exhibit 8: User Ratings: Security, Reliability/Uptime, Platform Support Options, and Costs



Several large company customers we spoke with mentioned that Microsoft's and IBM's endpoint management products had the "best out-of-the-box" reporting tools; while this stood out in our conversations, our survey respondents ranked reporting tools as relatively low in terms of key product endpoint management features. Our gap analysis revealed that Sentient Endpoint Manager rated best in key areas such as reliability and uptime, and rated well on cost of ownership and deployment. It scored lower in platform support options than IBM and Microsoft. Our conversations with Accelerite's customers revealed that this is due to the transitional phase with its native development of unified endpoint management capabilities, and support for newer mobile platforms being added.

Administration Requirements:

A challenge for many organizations is to staff appropriately for system administrators and those responsible for providing support services to PC users. Very frequently the system administration function is understaffed placing a greater premium on automation and standardization. The ratio of system administrators to PC users varies greatly and depends on the level of support required and the duration of support provided (i.e. 8-5 vs. 24/7). Typically leading organizations have ratios that range from 1:5,000 all the way up to 1:50,000 endpoints that support highly specialized and sophisticated applications and workflows. The higher ratios can be achieved through highly automated systems, and in deployment environments where users only require basic support service and are performing some level of self service.

While high availability of support services typically equates to higher levels of staffing requirements, there are best practices that can be employed to drive efficiencies. These range from automation of processes to strong documentation standards to the development of scripts or tools. Exhibit 9 depicts the primary factors that affect scalability and shows how deployment environment variance can impact administrator efficiencies.

Exhibit 9: Factors that Affect Scalability

Increased System Administrator Efficiency	Decreased System Administrator Efficiency
<ul style="list-style-type: none"> Common SA tools Tight control over what gets loaded on HW/SW baseline Redundancy of critical services Good training programs Centrally managed backup and restore program Hardware and software standards Robust security 	<ul style="list-style-type: none"> Diverse hardware baseline Diverse software baseline Lax security Separate dashboards and reports for different endpoint types Little to no training Reactive staff More manual/repetitive work and less automation

Optimizing labor expenses is critical, particularly for larger enterprise deployments. While each of the three platforms we compared have focused on automating administrative processes, our customer interviews and data showed that Sentient Endpoint Manager required fewer administrators per endpoint. This was in contrast to both IBM's and Microsoft's endpoint management products, which usually required additional administrators to update configuration details as managed deployment environments changed and expanded.

Conclusion

The market opportunity for mobility solutions has created a very fragmented, crowded, and competitive market. This is proving to be a challenge and puts a significant burden on CIOs and IT leaders who must evaluate, test, and experiment with competing approaches to manage their expanding mobile deployments alongside their traditional endpoints. Connectivity to enterprise resources including email, databases, and line-of-business applications is central to the value proposition of a well-integrated mobile solution securing connectivity is a fundamental requirement to manage risk of data leakage and unauthorized access. The strategy and policies for managing mobile endpoints should be consistent with those in place for desktop PCs and laptops. The rapid proliferation of smartphones and tablet computers is exposing corporate networks and information to unprecedented risk; this has made investments in securing mobile deployments of paramount importance. Players supporting Unified Endpoint Management are better placed to provide them with these capabilities more comprehensively than EMM point solution providers.

Accelerite's unified endpoint management offering meets the immediate and long-term endpoint management needs for medium to large deployment environments that require a breadth of endpoint management capabilities across traditional and modern device platforms. The solution's architecture and scalability delivers a lower cost of ownership, and the future mobile management enhancements the firm plans should enable it to continue to compete head-to-head with both Microsoft and IBM in the UEM space, and provide more comprehensive capability compared to pure-play EMM players.

Background on Accelerite

Accelerite is a provider of software, mobile, and cloud solutions to some of the largest enterprises in the world. Its products range from workload management and disaster recovery orchestration software to endpoint protection and management. Accelerite is the products business of Persistent Systems, a global leader in software product development and technology services, with over 7,500 team members worldwide.

Appendix A: Baseline Organization Description

Based on the results of an online survey and interviews with four large organizations that have extensive endpoint management investments, VDC constructed a baseline company. VDC created a financial framework in order to generate the potential return-on-investment (ROI) baseline analysis for organizations considering deploying enterprise-grade tools to track, manage, secure and troubleshoot PCs, laptops, mobile devices, and application usage throughout their business. This study illustrates the financial impact of deploying an endpoint management solution from leading endpoint management vendors by aggregating the findings from an online survey and through customer interviews; these data points have enabled us to portray a baseline organization that has

benefited from integrating an endpoint management solution into their IT service lifecycle processes and functions.

The baseline organization is a consumer packaged goods manufacturer, distributor, and service provider headquartered in the United States, with branch offices throughout Europe and the APAC region. The organization maintains 40 locations, has 12,500 employees and 20,000 endpoints (PCs, laptops, servers, and mobile devices) using approximately 500 software applications that are impacted by the deployment of an endpoint management solution. The company has a mature IT organization staffed with 150 employees, which operates as a shared service supporting global IT operations; the team administers, maintains, and manages PCs, laptops, servers, mobile devices, and applications across the enterprise.

Prior to implementing an endpoint management solution, the organization was using a variety of siloed point solutions to manage client, servers, applications, and mobile devices. The organization sought a single vendor that could replace these products and provide an integrated and unified console to manage assets, inventory, application provisioning, mobile devices, and IT Service Management frameworks.

Disclosures

The reader should be aware of the following:

This study was commissioned by Accelerite and delivered by VDC Research. VDC makes no assumptions as to the potential return on investment that other organizations will receive.

Accelerite reviewed and provided feedback to VDC, but VDC maintains editorial control over the study and its findings and does not accept changes to the study that contradict VDC's findings or obscure the meaning of the study.

Disclaimer

Every organization has unique considerations for economic analysis, and significant business investments should undergo a rigorous economic justification to comprehensively identify the full business impact of those investments. This analysis report is for informational purposes only. VDC strongly advises that readers should use their own estimates within the framework provided in the report to determine the appropriateness of an investment in an endpoint management solution. Product names, logos, brands, and other trademarks featured or referred to within this report are the property of their respective trademark holders in the United States and/or other countries.

VDC Research MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. ©2015

VDC Research

About the Author

ERIC KLEIN is a market research and consulting professional specializing in the design, analysis, and delivery of project-based research. Over the past 15 years, Eric has worked with a wide array of firms across a number of industries, leading quantitative and qualitative research in areas such as innovation in enterprise software, supply chain risk management, manufacturing operations/automation, and IT spending research. Eric has worked in a variety of market research and management roles, providing market data and competitive intelligence to Fortune 500 firms. His previous employers include: AMR Research, The Yankee Group, and Affiliated Computer Services (ACS). Eric holds a Bachelor of Science in Finance from Boston University

Contact Eric:

eklein@vdcresearch.com

DAVID KREBS has more than ten years experience covering the markets for enterprise and government mobility solutions, wireless data communication technologies and automatic data-capture research and consulting. David focuses on identifying the key drivers and enablers in the adoption of mobile and wireless solutions among mobile workers in the extended enterprise. David's consulting and strategic advisory experience is far reaching and includes technology and market opportunity assessments, technology penetration and adoption enablers, partner profiling and development, new product development and M&A due diligence support. David has extensive primary market research management and execution experience to support market sizing and forecasting, total cost of ownership (TCO), comparative product performance evaluation, competitive benchmarking and end user requirements analysis. David is a graduate of Boston University (BSBA)

About VDC Research

Founded in 1971, VDC Research provides in-depth insights to technology vendors, end users, and investors across the globe. As a market research and consulting firm, VDC's coverage of AutoID, enterprise mobility, industrial automation, and IoT and embedded technologies is among the most advanced in the industry, helping our clients make critical decisions with confidence. Offering syndicated reports and custom consultation, our methodologies consistently provide accurate forecasts and unmatched thought leadership for deeply technical markets. Located in Natick, Massachusetts, VDC prides itself on its close personal relationships with clients, delivering an attention to detail and a unique perspective that is second to none.

For more information, contact us at info@vdcresearch.com.