

# Choosing the Best Mobility Management Solution

## TCO, Satisfaction, Data Protection and Security



Exclusive License  
to Distribute

 **BlackBerry**

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

# INSIDE THIS REPORT

VDC Research conducted a comparative analysis of the mobility management, data protection and security capabilities of BlackBerry's unified endpoint management (UEM) solution and Microsoft's Intune UEM solution. Each was assessed on the level of assurance and utility they provided, their cost effectiveness/total cost of ownership (TCO), and their impact on user experience. Our analysis included an in-depth review of product documentation as well as interviews with both BlackBerry and Microsoft customers.

VDC surveyed 208 IT decision makers (ITDMs) that were responsible for overseeing end-user computing for their organization. Our research included OS usage and migration trends, endpoint device trends, such as UEM, and their effect on the entrenched end user computing (EUC) ecosystem — namely, Windows-based PCs. Hardware, software, and cost information were provided by both BlackBerry and Microsoft; 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.

Our survey respondents were based in North America, with roughly two-thirds working in high tech manufacturing, financial services, industrial manufacturing, retail and healthcare industries. Other industries represented included: government, transportation/wholesale distribution, media and communications, automotive, chemical and consumer products manufacturers. 57% worked in organizations with 250-4,999 employees and 43% worked in organizations with more than 5,000 employees. This vertical focus was built in by design, given the complex endpoint environment driven in part by adoption of endpoint management solutions. The demographics of our survey are provided in the Appendix of this whitepaper.

This whitepaper will detail the changing nature of end-user computing deployment environments, discuss the need for modern mobility management and collaboration tools that provide secure access to SaaS, web, mobile, Windows, and Linux apps, as well as desktops and access to corporate data. It will assess how market leading vendors (specifically, BlackBerry and Microsoft) are bundling their modern mobility management solutions and assess the direct and indirect costs of these bundled solutions.

## WHAT QUESTIONS ARE ADDRESSED?

- > Why you should pay close attention to the growing ranks of users that rely on mobile data and app access
- > How BlackBerry and Microsoft differentiate on native security and compliance
- > How BlackBerry and Microsoft have evolved their modern UEM solutions
- > How the TCO of BlackBerry and Microsoft's modern mobility management solutions differ
- > Why best-of-breed vs. platform and vendor lock-in remain relevant in today's technology deployments

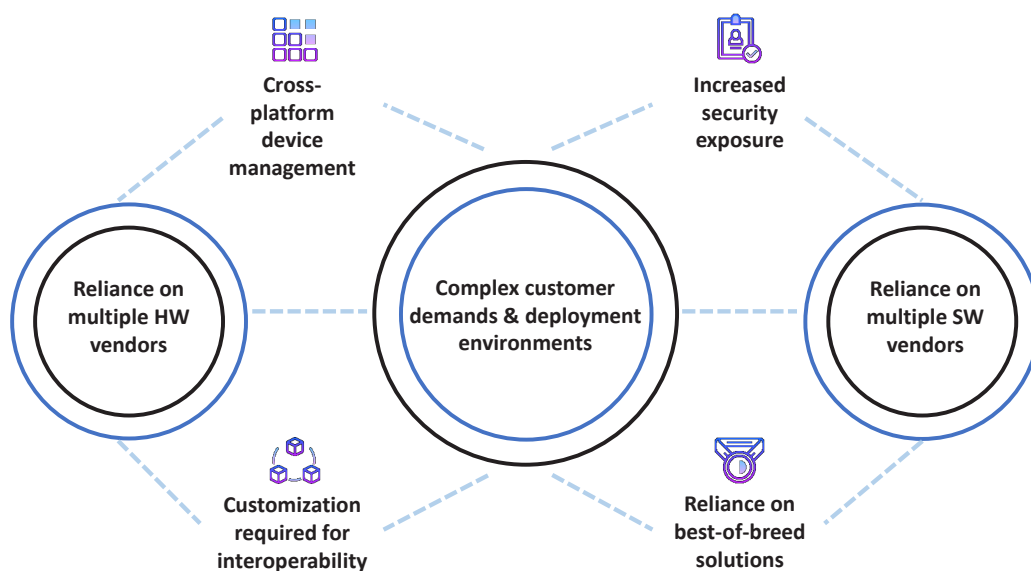
## WHO SHOULD READ THIS REPORT?

Anyone participating directly or indirectly in the development, marketing, or distribution of solutions to manage end-user computing deployment environments is a suitable audience. This report summarizes key market trends related to modern mobility management and the cost/technology effectiveness of market leading solutions; ultimately, this report is intended to educate the reader about the core elements of BlackBerry and Microsoft's modern UEM mobility management solutions.

# MOBILITY MANAGEMENT EVOLUTION

The changes occurring in end-user computing environments have been incremental since PCs became a fixture at every business user's desk; but, "keeping the lights on" from an IT perspective continues to grow more complex. With implementations of analytics and machine learning growing more sophisticated, many organizations now possess quantitative data that proves that avoiding downtime is just the beginning of their IT modernization journey. These trends have many organizations actively making technology investments to improve customer engagement and to offer new services to their customers and partners. This is why mobile enablement has become business-critical within industry sectors such as retail and hospitality, transportation and logistics, and warehouses and distribution centers. Not only have user expectations changed, teams are more diverse and globally distributed, and mobile enablement is exacerbating the threat environment. Exhibit 1 shows the current realities of today's complex mobile estate.

*Exhibit 1: Today's Mobile Estate*



The traditional boundaries of the 9-to-5 workday — in terms of time and location — no longer apply. Collaboration across workspaces, devices, and geographical locations has become the norm for today's connected workforce, and the boundaries of where, when, and which device we expect to be able to work with has continued to shift. People work on projects before and after work, during their commutes, at community events — even while on vacation. As such, work needs to flow seamlessly across time, location, and devices. But, transitioning to an era of scalable architectures, business-critical web services, customer-facing applications, and mobile-enabled workforces come with complexities. While these challenges are not unique, they have made capitalizing on technologies that can help automate and optimize business processes and user experiences complex.

While every organization is different in terms of its reliance on technology, the rise of the Chief Digital Office (CDO) role has occurred as a result of several unmistakable trends. Demands for cross-platform mobile enablement, business agility, high performance and high availability have added complexity to what are already challenging IT deployment environments. This, in turn, has made effective IT and digital leadership more important today than it has ever been. But modern endpoint management software is but one element in the broad range of complementary technologies that have quickly become business-critical infrastructure components. While this has led to IT having to support a multi-vendor, multi-OS, and multi-console environment, this has not only become the norm, but has allowed organizations to augment their security postures and customize their environments to their own unique requirements. This type of approach is necessary in any organization that is regulated or in government deployment scenarios. In addition, the rising threats of malware, phishing and other data-exfiltration schemes has made augmenting mobile security a growing concern across all industry sectors due to financial and reputational damage security breaches can levy.

## Baseline Organization

VDC created a financial framework in order to generate the potential return-on-investment (ROI) baseline analysis for organizations considering deploying a cloud-based UEM solution to track, manage, secure and troubleshoot their disparate and increasingly mobile end user computing deployments. This study illustrates the financial impact of deploying a modern mobility management solution from leading mobility 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 a UEM solution into their IT service lifecycle processes and functions.

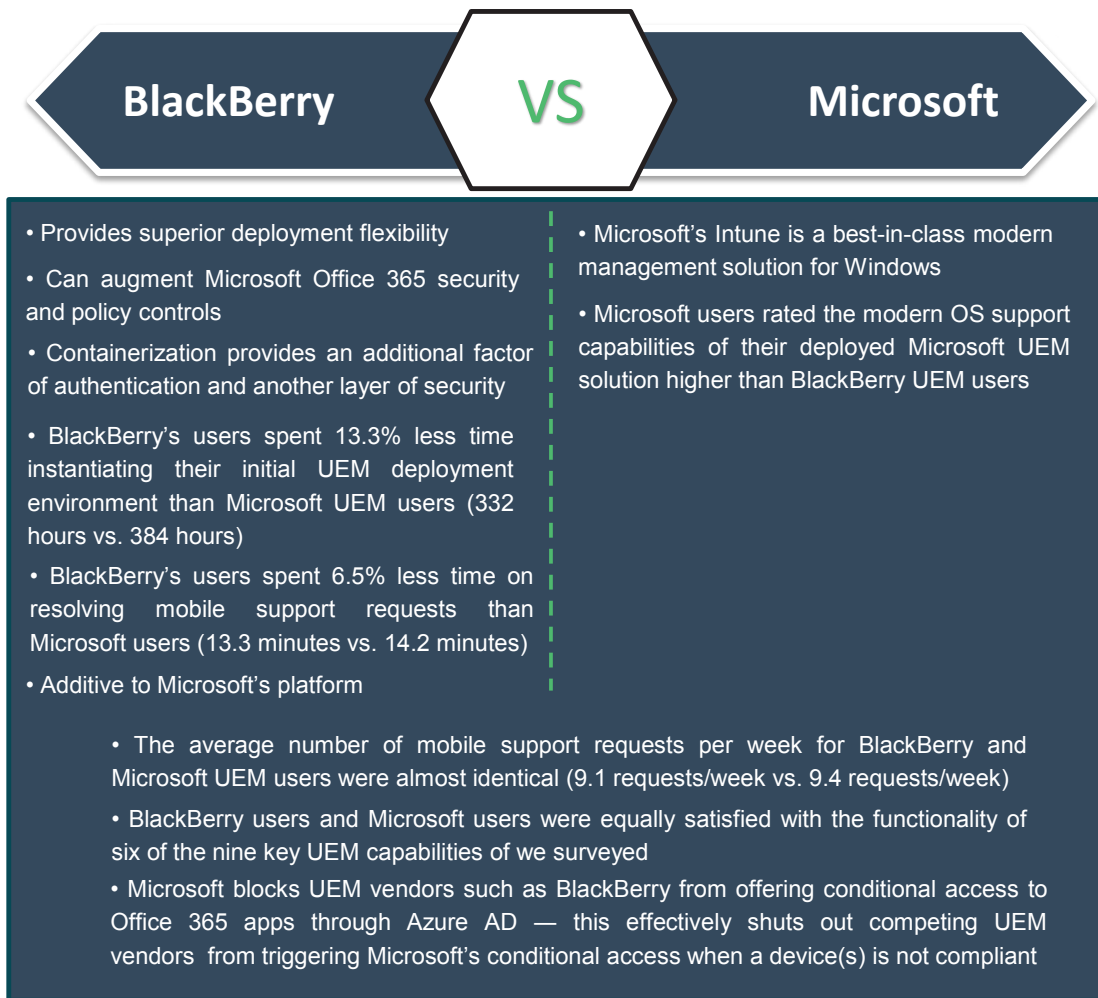
The baseline organization is regulated and is a private company; it is headquartered in the United States with branch offices throughout Europe and the APAC region. maintains 35 locations, has 20,000 employees and 50,000 endpoints (spanning mobile devices, desktop PCs, laptops, and servers) — approximately >300 software applications have been deployed (Office 365 being one of said applications) some of which are impacted by the deployment of a UEM solution, and 15,000 mobile devices (a mix of iOS and Android) that require modern mobility, application and content management software licenses in a BYOD and corporate-owned personally-enabled (COPE) deployment environment. Independent verification of the security, privacy, and compliance controls of its endpoint management solutions are required, and device management policies must be geared to high trust and verification. Finally, it 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 a UEM 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 several of these products and provide an integrated and unified console to manage assets, inventory, application provisioning, mobile devices, and IT Service Management frameworks.

## UEM Deployment Details

Enterprise connectivity workload	High (500 kbps)
Security audit logging requirements	High
Deployment size	Large (15,000 mobile devices)
% of workforce with 'premium' mobile enablement (e.g., multiple containers, extensive application options (including Office 365)	15-20%
Ownership model	Mix of BYO and Corporate provisioned
Device management workload	Heavy

VDC analyzed the economic benefits of deploying a cloud-based modern mobility management solution in the deployment environment described in the baseline organization from BlackBerry (UEM 12.10) and from Microsoft (Microsoft 365). Each was assessed on the level of assurance and utility they provided, their cost effectiveness/total cost of ownership (TCO), and their impact on user experience. Factors such as the complexity of the applications used, ownership models supported (e.g., BYO, COPE, COBO, etc.), IT labor, the level of support users require, and the impact mobile devices on user productivity were core elements of our TCO model. Exhibit 2 summarizes our key findings.



## UEM BECOMES BUSINESS-CRITICAL

There are several EUC trends that require additional security mechanisms to be implemented; particularly in larger corporate deployments such as the aforementioned baseline organization we described. User expectations have evolved, business applications and core IT infrastructure elements have moved to the web and to the cloud, and larger portions of mobile deployments are becoming business-critical. These trends make native control of data wherever it is (at rest or in motion) a priority — particularly for any regulated industries such as financial services, healthcare and in government-related mobility deployments.

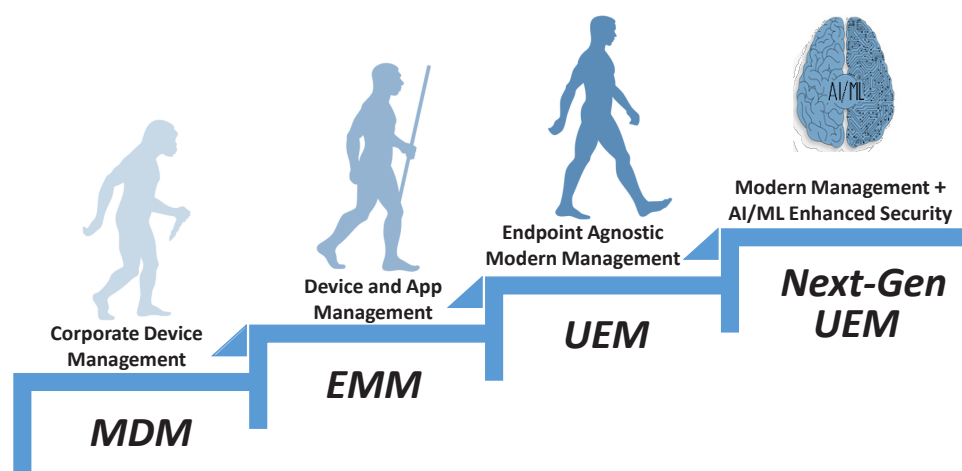
Modern mobility management has evolved from a specialized mobile device-centric configuration platform to a broader role, managing, securing, and enforcing policy on a wide range of endpoints, from mobile devices to PCs and smart connected enterprise IoT endpoints. Strong adoption of the technology among U.S. enterprises is reflected in double-digit growth in market revenue over the past several years. UEM is a single software platform that controls both PC, mobile, and IoT endpoints. According to a recent VDC survey, more than 40% of organizations have deployed mobility management solutions for some of their PC management requirements, and more than a quarter are using these solutions for IoT-centric use cases. Interest in UEM is being driven by the desire to enhance IT productivity, simplify support and administration, and improve security posture while reducing licensing costs. These solutions are becoming more strategic to every business and play an outsized role in business-critical mobility deployments where they have become indispensable to the daily workflows.

## Why UEM TCO Matters

Securing mobile devices (protecting data through encryption and passcode policies, locking down certain device features, auditing devices, etc.); managing mobile devices (asset and inventory management, updating and provisioning new policies, pushing out new configuration policies, etc.); and deploying mobile devices (activating devices, enrolling them in policies, authenticating users, configuring policies, provisioning apps, etc.) are the core competencies of these solutions. But, the advent of BYOD means that solutions must not only be endpoint agnostic, but also be able to compile telemetry data from all potential sources across network elements, including headless devices such as connected IoT endpoints – these remain areas for differentiation in the UEM market.

Going forward, UEM solutions will become core infrastructure elements that can augment an organizations security posture while optimizing application access, usability and reliability — this in turn can help to reduce support costs and keep a mobile workforce engaged and efficient. Exhibit 3 shows the evolution from MDM to UEM.

*Exhibit 3: MDM's Evolution*



Mobility management solutions have become core IT infrastructure elements, and have become indispensable for managing device lifecycles, as well as in automating time consuming administrative tasks such as onboarding and decommissioning users. Furthermore, BYOD trends have made the ability to customize user groups and assign access privileges, configurations, and application availability based on job function or role essential for many organizations (our survey showed that 84% of BlackBerry and Microsoft UEM solutions required support multiple device ownership models). MDM solutions have evolved from basic device protection to enabling and protecting mobile apps and services (EMM) to expanding modern management techniques to the desktop (UEM). Ultimately, UEM solutions are acquired to streamline the administration, management, maintenance and support requirements of today's increasingly mobile-dependent workforce.

VDC's research shows that more than half of all employees in the United States and Europe work outside of a traditional office — be it from the road, a client site, or a home office. But to be successful in supporting these remote work scenarios, employees must have the tools they need to stay in touch with their colleagues and customers. Access to data repositories and collaboration tools that can run on any device are essential. These tools are critical for employee satisfaction and job retention, both of which can deliver a competitive advantage. Both BlackBerry and Microsoft's UEM solutions can streamline the administration of the required solutions that can solve these issues and can drastically simplifying the following key tasks to support such remote work scenarios:

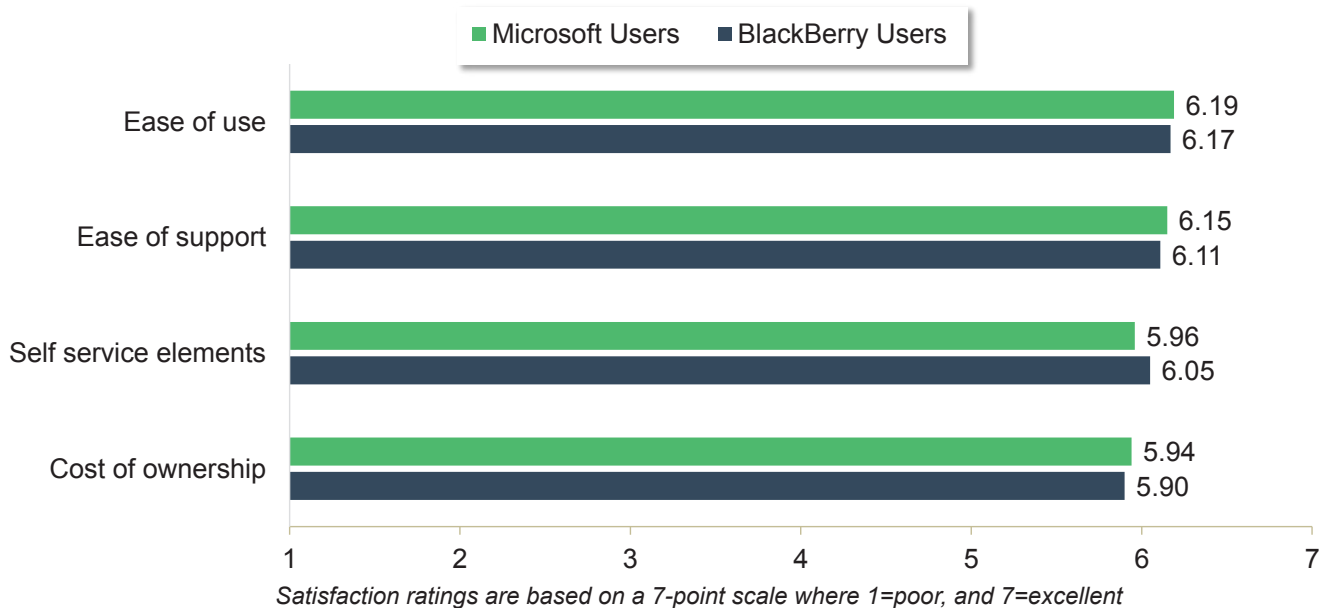
- > Device Enrollment: Setting up accounts for online app store access (Apple & Google)
- > Device compliance: Setting device polices for the secure access to corporate data
- > Device configuration: Setting up policies for device management
- > Mobile Apps: Managing device-side applications
- > Conditional Access: Controls on accessing corporate data on devices



# BLACKBERRY VS. MICROSOFT POSITIONING

BlackBerry: BlackBerry's modern mobility management portfolio is centered on a well-integrated suite of mobile device, application and content management capabilities, combined with strong security features. Designed for both managed and unmanaged device scenarios, BlackBerry's Unified Endpoint Manager (BlackBerry UEM), provides strong device management configuration and security capabilities that reflect the company's tenure as one of the original enterprise-scale MDM solution providers. BlackBerry's apps provides secure and easy access to corporate email, calendars, contacts, presence, and document access/editing. While BlackBerry always possessed strong application management capabilities, its prowess in making strategic acquisitions (Good Technologies and WatchDox were instrumental in this regard) have it well-positioned to compete in what have become a competitive UEM market with increasing vendor parity. Our Survey data confirmed this; Exhibit 4 shows users' satisfaction with their currently deployed UEM solution.

*Exhibit 4: Current Overall End User Satisfaction With BlackBerry and Microsoft's UEM Solutions*



While user satisfaction with BlackBerry's solution was slightly higher than Microsoft, the variance was not statistically significant. BlackBerry does possess differentiation with its containerized workspace (called BlackBerry Work) which performs well in deployment environments that support unmanaged devices — particularly in deployments where multiple apps must be containerized. Network activity for containerized apps can be directed into several secure web gateway (SWG) and app reputation vendors and approved third-party apps are tested, signed and are guaranteed to be certified when downloaded from commercial app stores.

BlackBerry's content management solution (a cloud-based file sync and share offering called Workspaces built on WatchDox IP) performs well on Windows 10 and mobile platforms and offers robust security, data confidentiality, and digital rights management. The company's UEM solution delivers a single integrated view of users, devices, apps and policies on mobile platforms as well as Windows 10 and macOS. In addition, the solution can be highly customized, but can be difficult to configure initially (which appears to be normal in the UEM software category). Finally, BlackBerry's SSO solution unifies and simplifies cloud service access and entitlement with Active Directory integration, PKI integration, Kerberos and SAML support for browser access.

**Verdict:** Our survey and analysis indicated that BlackBerry UEM customers have had success in reducing IT labor (the flexibility and usability of the UEM administrative console has both evolved and improved) as well as ongoing administrative burdens once the solution is appropriately configured and optimized. Customer interviews confirmed this. BlackBerry's UEM solution also performs well in enabling a diverse set of personas (e.g., executive, managerial, frontline workers, contractors, etc.) for all ownership models, and delivers on enhancing end user productivity and collaboration (with Office 365 access enabled). Users that have deployed BlackBerry's UEM like the solutions native productivity applications (Work, Notes, and Tasks) — the solution also provides IT with a means of enforcing granular policy control while providing access to behind the firewall intranet applications as well as cloud applications. Finally, BlackBerry's acquisition of Cylance has the vendor well-positioned to integrate behavioral analytics into its UEM solution — we expect to see this integration occur in late 2019. Once the integration of Cylance behavioral analytics solution is complete, BlackBerry will be able to offer big data, predictive/behavioral analytics and cloud services to its customers.

BlackBerry core differentiation remains in deployment environments where security, privacy and compliance are required — particularly regulated industries such as healthcare, financial services and in government deployments. BlackBerry's solution incorporates encryption for Android, iOS and Windows platforms, and its UEM solution features native support for market-leading 2FA solutions, containers can be bound to additional local authentication mechanisms (useful in government and in military deployments) such as multifactor authentication (including biometrics) and hardware-level security platforms such as ARM's TrustZone and Intel's SGX that use hardware-based isolation and memory encryption techniques. BlackBerry's certifications (e.g., FIPS 140-2, Common Criteria and FedRAMP) give it a significant advantage in highly-regulated industries and in government and military deployments.

BlackBerry has also developed important differentiation around application access. The company's UEM solution provides a much simpler path to enabling end users with access to both custom and/or third-party applications. This is counter to Microsoft's approach which limits application choice and focuses on Microsoft's collaboration suite/apps. BlackBerry's focus on developing more extensive ISV partnerships with deeper integrations is critical to promoting end user productivity. While more can be done around improving email workflows — particularly workflows that involve app access — BlackBerry is ahead in this regard.

Our analysis concluded that there was significant feature parity between BlackBerry's and Microsoft's UEM solutions head-to-head. But BlackBerry's NOC-based architecture offers differentiated embedded security and provides strong cloud-based connectivity to internal apps and assets without requiring complex VPN and firewall configurations; in addition, organizations supporting BYO ownership models will find that BlackBerry requires fewer MDM policies to support iOS, Android, and Samsung Knox deployments. Finally, for organizations looking to deploy mobile threat detection (MTP), MTP setup for market leading solutions from vendors such as Lookout, Symantec and Zimperium is relatively seamless on both BlackBerry and Microsoft's UEM solutions. As would be expected, BlackBerry lags Microsoft in possessing functionality and tools to help transition customers from legacy PCLM tools to modern management or co-management scenarios; however, these capabilities are being considered. But ultimately, organizations will need to transition away from legacy on-premises PCLM tools as they fall short of new OS and remote workforce demands. Going forward, the traditional IT model of using different point products for different endpoints is both ineffective and inefficient.

**Microsoft:** Microsoft has perennially struggled with its mobile initiatives; it's acquisition of Nokia's handset business failed, and Windows Phone devices never gained traction in the market. But, the company has made it very clear that it now sees modern mobility management as a core element to its B2B solutions. Microsoft's Intune is a central element of this strategy. While Intune was originally designed as a slimmed down version of System Center Configuration Manager for smaller organizations with a mobile workforce, Microsoft quickly recognized that expanding Intune to manage Android and iOS devices (along with legacy and modern Windows devices) was required to compete in the UEM market.



Since its release in 2014, Microsoft has augmented its core assets and has worked hard to elevate the messaging around its UEM platform which is marketed as Microsoft 365. Intune has become a core element to Microsoft 365; it integrates closely with Azure Active Directory (Azure AD) for identity and access control, and Azure Rights Management (Azure RMS) for data protection. Intune serves as the management element of Microsoft Enterprise Mobility + Security (EMS), and Office 365 is the productivity arm of Microsoft's mobility solution — each is foundational to Microsoft's overall UEM strategy.

**Verdict:** Microsoft is well aware of the changes occurring in customers' deployment environments; the company's Windows 10 OS has been widely adopted and offers modern management capabilities as well as many notable native security enhancements. Specifically, Microsoft delivers comprehensive data protection and robust security controls that protect the physical endpoint and the cloud. The company's tenure in end user computing has helped the company maintain a dominant position in the enterprise productivity and identity management markets. In addition, a wide majority of enterprise customers rely heavily on core Microsoft infrastructure components (e.g., Exchange, Office, and Azure Active Directory).

Microsoft's UEM solution is cloud only, which eliminates it as an option for organizations that require an on-premise UEM solution. Microsoft's UEM solutions lacks security certificates and is unable to deliver a government-grade solution or validated encryption). But, for Windows 10 devices; Microsoft's Intune is a best-in-class modern mobility management solution with well-integrated native security. By using a hardware security module for encryption and Windows Information Protection (WIP), Microsoft can very effectively manage business data without the need for containerization or app wrapping. But, mobile devices are a different story. Microsoft has yet to implement an effective means of extending conditional access outside of its Azure Cloud and preventing untrusted apps from accessing corporate data.

By making Intune essential to access certain key features and security controls of Office 365 and Azure AD, Microsoft has effectively given Office 365 users who have already invested in a UEM solutions such as BlackBerry's UEM an ultimatum — migrate to Intune or degrade your security and user experience. While Microsoft reluctantly began letting competing UEM vendors gain access to Intune's app protection policies (Intune APIs for Microsoft's Graph API were made public in 2018) and only provides Intune users with the ability to offer conditional access for Office 365 through Azure AD. This effectively shuts out competing UEM vendors from triggering Microsoft's conditional access when a device(s) is not compliant.

Finally, BlackBerry has achieved certifications for Common Criteria EAL4+, and Federal Information Processing Standardization (FIPS) 140-2 Level 1 for its UEM solution. The vendors' ability to offer seamless and contextual (e.g., by job function, location, network connection type and time) policy enforcement across different device types is unique in the UEM market.

## Better Together

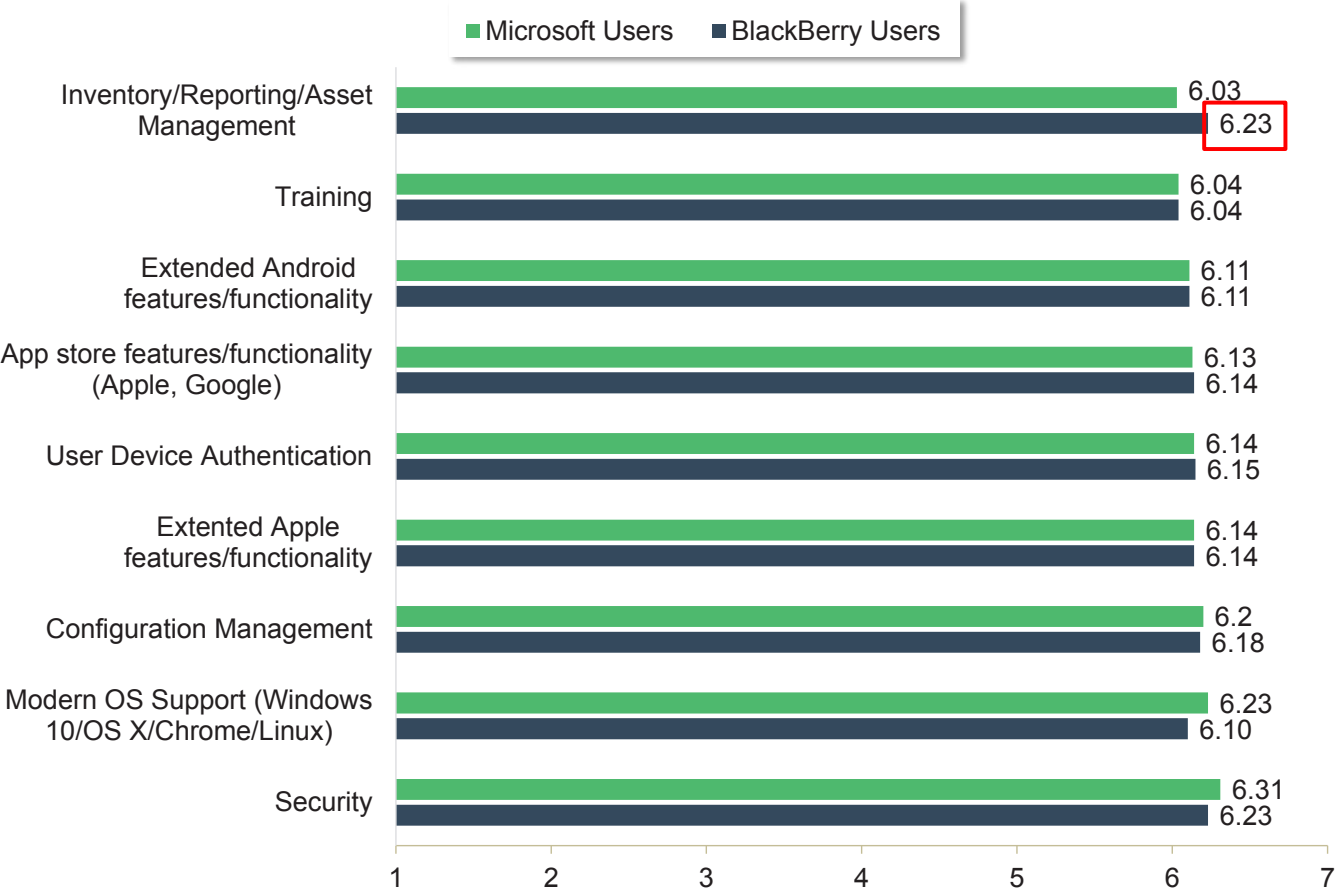
The shift to cloud infrastructure offers a wide range of advantages relative to on-premises alternatives, including financial benefits, significantly reduced administration and overhead, a more frequent and less disruptive update cycle, and radically expanded capacity and scalability. Hybrid (mixed on-premises and cloud) infrastructure will be the dominant enterprise infrastructure pattern for the immediate future, but content and collaboration investments are rapidly shifting to cloud service providers; productivity suites such as Microsoft's Office 365 and Google's G Suite figure prominently in these deployment scenarios, but there are important factors to consider when supporting these platforms. Specifically relating to endpoint security which remains as a barrier to broader adoption of cloud technologies.

As more organizations embrace multi-vendor public, private, hybrid cloud deployments, native control of data wherever it may reside has become increasingly important. BlackBerry's UEM solution can help to reduce data leakage scenarios that are routinely exposed by Office 365 and can be additive to Microsoft infrastructure for a variety of reasons:

- > The security and usability of Windows-based devices and Microsoft applications can be enhanced through existing integrations with Azure Active Directory, Office 365, Microsoft Intune, Windows 10 and other key Microsoft technologies.
- > Office 365 data leakage scenarios can be minimized, and security posture by enforcing PIN access to applications and restricting cut/copy/paste between Office and non-Office apps.
- > Disable “save as” scenarios where corporate data can be saved to personal file repositories such as Box/ Dropbox.

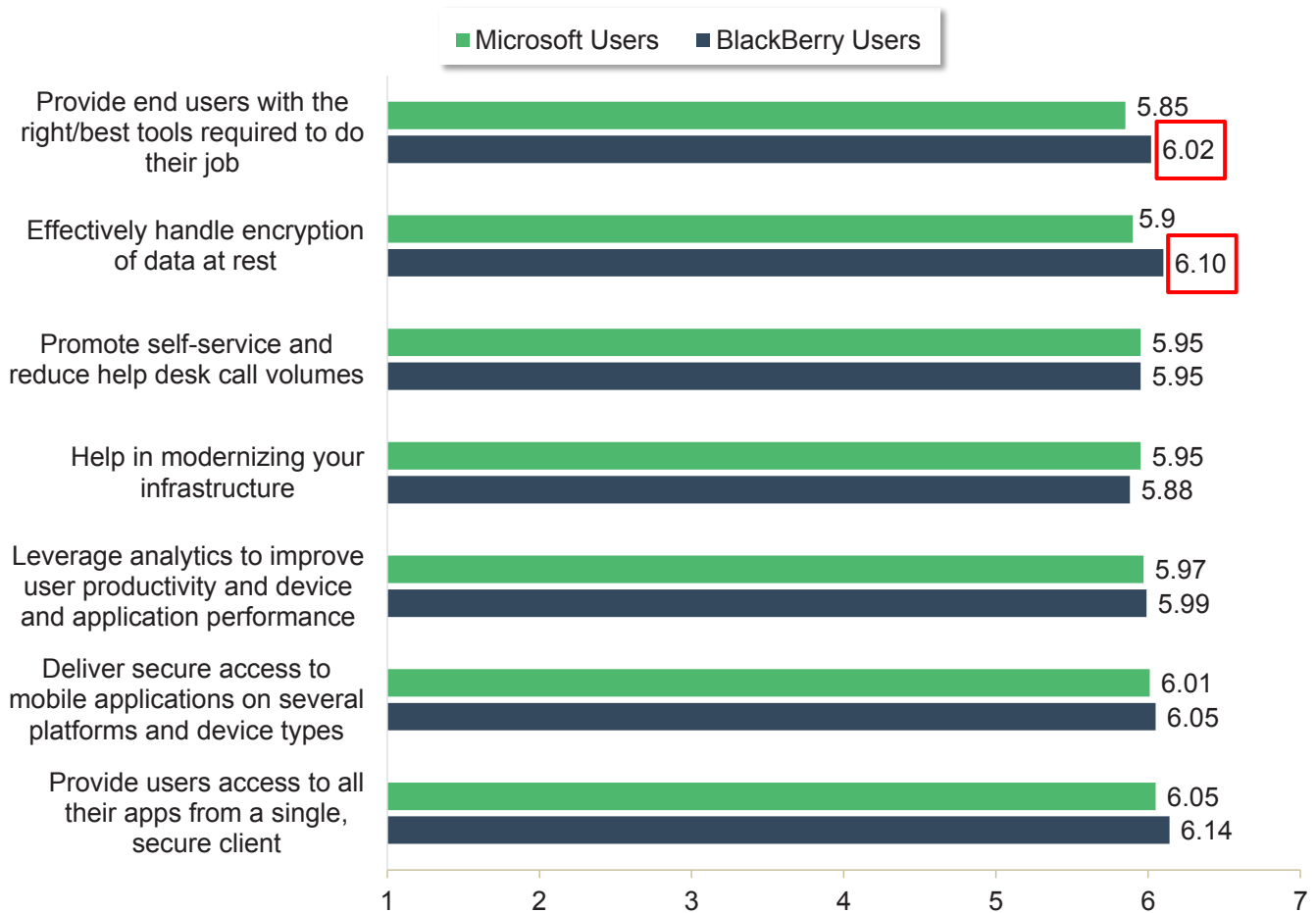
Ensuring users are sufficiently enabled and equipped from a device perspective (as described in our baseline organization) has mobility becoming a Tier 1 service that requires the ability to enforce comprehensive security mechanisms and deliver reliable access to corporate data and applications. For this reason UEM solutions that are competitive with Microsoft can help to simplify the infrastructure elements of a deployment while reducing its attack surface. By integrating with Intune's application protection mechanisms, vendors such as BlackBerry can augment security and policy controls for Microsoft Office 365 while providing IT with deployment flexibility that Microsoft is currently unable to achieve. Table 2 shows BlackBerry and Microsoft users' satisfaction with core UEM features.

Exhibit 5a: Satisfaction with Specific UEM Solution



Red box indicates areas where there was statistical significance  
Satisfaction ratings are based on a 7-point scale where 1=poor, and 7=excellent

Exhibit 5b: Satisfaction with Currently Deployed UEM Solution



Red box indicates areas where there was statistical significance  
Satisfaction ratings are based on a 7-point scale where 1=poor, and 7=excellent

## Cost Avoidance Opportunity

In today's service driven economy, an organization's greatest asset — and cost — is in its workforce and their time. Optimizing this time is crucial to many organization's operational strategy and has led increasing investments mobile enablement. VDC's research has consistently shown that mobile enablement initiatives have focused on very specific areas: these are improving customer service and engagement, reducing costs, and increasing productivity. What has become clear over this period is that supporting the mobile devices of larger fleets has led to more complexity and often more headaches for IT. Managing the mobile lifecycle of these fleets has been a perennial challenge; in addition, mobile endpoints must not only be properly secured, applications must also be provisioned/managed.

Minimizing the impact of failure of business-critical mobile solutions can be easily achieved with the UEM solutions from both BlackBerry and Microsoft; each can improve operational visibility of your mobile estate, and have robust capabilities for remote device/content/application management.

The cost avoidances that are available can be significant — the elimination of software upgrade and patching alone can significantly provide labor and staging savings. In high-security deployment environments these are an exception, as the initial optimization and integration work specific to security is likely to add labor costs, due to need for security specialists perform the appropriate test, certifications and system configurations.

# CONCLUSIONS

The desire by enterprises to change and streamline how PCs and mobile devices are deployed, imaged, updated, provisioned, secured and managed combined with external factors such as the rapid shift towards cloud-based enterprise applications has made investment in a UEM solution a requirement for large regulated organizations. Cloud-native UEM solutions such as BlackBerry's and Microsoft's offer opportunities for IT to support more flexible operations while providing their users with simplicity and robust security from boot up to shut down. These UEM solutions have the potential to transform the way organizations collaborate, access applications, and get work done. While most organizations are well aware of the benefits of cloud computing, UEM solutions can help to promote business agility and flexibility by streamlining cross-platform access to corporate content and applications. Modern UEM solutions can play an outsized role in EUC deployments as these environments continue to evolve.

The attack surface on mobile platforms is broad (Bluetooth, NFC, WiFi, GPS, etc.), and the pocketable nature of mobile devices makes possessing the ability to remotely lock down and wipe devices critical, particularly for end users with access to corporate data and applications. Mobile devices are vulnerable to malware and viruses, UEM solutions are powerful, but require complementary solutions to expand the exploit mitigation and threat intelligence capabilities and elements of their platforms. Most organizations not only run multiple OSs, but are supporting a variety of form-factors, apps, identity providers, and cloud services; and, they want to harden their security posture through layered security. BlackBerry's architecture and ISV partner strategy is better aligned for this reality than Microsoft who well down the path of positioning its venerable Office franchise and cloud services to influence enterprise computing decisions outside its productivity suite.

Both BlackBerry and Microsoft's UEM solutions offer the potential to transform the way organizations collaborate, access applications, and get work done. Most organizations are well aware of the benefits of cloud computing — agility, flexibility and cost savings are provided by the ability to securely consume infrastructure and platform services on demand without a large capital injection is proven. These benefits can be gleaned to various degrees from implementations of any or all the components of a hybrid cloud, including virtualization, private cloud and public cloud. But, while the business case for implementing any or all of these solutions is not difficult to build up, many digital transformation initiatives lack the inherent security elements a modern UEM solution can offer. While both BlackBerry and Microsoft have developed robust and native security elements, our analysis showed that these solutions are better when deployed alongside one another — this is especially the case in organizations similar to the baseline organization we outlined in this report. BlackBerry's containerization provides an additional factor of authentication and another layer of security that can help to keep corporate data safe even if a device's passcode and/or encryption are compromised. This technique can also help to ensure that only appropriately authenticated devices and users gain access to their provisioned business applications.

BlackBerry's has figured prominently in high-security deployment environments (e.g., military, government and non-government industries such as financial services, healthcare) which require the highest levels of legal compliance. The company has achieved certifications for Common Criteria EAL4+, and Federal Information Processing Standardization (FIPS) 140-2 Level 1 for its UEM solution. The vendors' ability to offer seamless and contextual (e.g., by job function, location, network connection type and time) policy enforcement across different device types is unique in the UEM market. The company's security bona fides make it a very good choice for organizations that require robust security for certain segments of their workforce (e.g., BYOD) while providing the ability to enable high-security for other users. Finally, BlackBerry's architecture can provide important countermeasures to enhance the security bona-fides of Microsoft's platform. These integrations offer a means of countering data exfiltration, malware/phishing and augmenting the overall security posture of cross-platform deployment environment. But, deploying, integrating, and managing a mix of third-party tools (e.g., mobile threat defense, network access control and secure web gateways) can not only add complexity to a deployment, but can be detrimental to user experience, and can potentially increase the TCO and an UEM deployment.

## Disclosures

The reader should be aware of the following: This research was commissioned by BlackBerry and delivered by VDC Research. VDC makes no assumptions as to the potential return on investment that other organizations will receive. BlackBerry 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. ©2019

# ABOUT THE AUTHORS



Eric Klein

**Eric Klein** is a market research and consulting professional who specializes 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 degree in finance from Boston University.

## Contact Eric:

[eklein@vdcresearch.com](mailto:eklein@vdcresearch.com)



David Krebs

**David Krebs** has more than 10 years of 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).

## Contact David:

[davidk@vdcresearch.com](mailto:davidk@vdcresearch.com)

# 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.

**VDC Research**  
Insights for the Connected World

© 2019 VDC Research Group, Inc. | P 508-653-9000 | [info@vdcresearch.com](mailto:info@vdcresearch.com)