Unified Endpoint Management: Enabling Responsible End-User Computing in a Multi-Device World

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM
March 2018
# Table of Contents

- Executive Summary ................................................................................................................................. 1
- The Evolving Landscape of End-user Computing .................................................................................. 1
- The Rising Need for Endpoint Management in a Multi-Device World ................................................. 2
- Empowering Users with Unified Endpoint Management ........................................................................ 5
- Enabling Effective Unified Endpoint Management ................................................................................. 7
- EMA Perspective ...................................................................................................................................... 9
- About IBM Security .................................................................................................................................. 10
Executive Summary
As organizations accelerate their reliance on an increasing number of endpoints—including smartphones, tablets, laptops, desktops, wearables, and the Internet of Things (IoT)—IT organizations are increasingly challenged to support end-user needs while continuously meeting business and security requirements. Traditional endpoint client management processes principally designed only to support Windows devices (such as configuration management, patch distribution, software update management, and image-based provisioning) are no longer sustainable and fail to address today’s more complex application and data storage ecosystems. Unified endpoint management (UEM) solutions consolidate the management, security, and provisioning processes for endpoints deployed to perform business tasks regardless of their type, location, or ownership. Adopting a responsible UEM approach will result in enhanced security assurance, reduced management efforts and related costs, and improved workforce productivity and satisfaction.

The Evolving Landscape of End-user Computing
When IBM coined the term “personal computer” (PC) in the early 1980s, it was in reference to a computing device that could be used by just one person—in contrast to terminal-based servers, mainframes, and supercomputers that were utilized simultaneously by many users. Little did the pioneers know just how personal these PCs would ultimately become. Fast forward to today, there’s a dizzying array of devices to choose from, and they are versatile enough to be used for work and personal purposes, chief among them communications, personal management, entertainment, and everyday job tasks. The decision of which types of devices to use for which purposes is, in most cases, entirely dependent on the user’s personal preference. This change in the device selection processes led to a “consumerization of IT” that empowered users as never before to interact with different kinds of technology best suited to meet their unique styles, requirements, and capabilities.

For businesses and other professional organizations, the broad influx of new and different device types introduced by their workforces has been something of a double-edged sword. Certainly personalized device selections have greatly increased workforce productivity and job satisfaction rates, but they have also introduced complex IT management requirements for enabling multi-device support. According to EMA primary research, more than half of all business professionals regularly perform job tasks on more than one type of device, and trending patterns suggest this ratio is rapidly increasing as users also utilize wearables (smartwatches, smart glasses, etc.) and IoT devices. In the process, the number of devices IT managers need to track, secure, and support has increased exponentially, increasing the number of adjacent management responsibilities proportionally. For instance, for each device administrators need to identify appropriate applications, network requirements, security vulnerabilities, and system limitations so that corresponding processes and solution can be introduced.
It is important to recognize that accelerating requirements for multi-device support are not just applied to an increasing number of hardware platforms, but also to a much more diverse set of operating system environments (figure 1). For instance, the business adoption of macOS devices has more than doubled over the last three years, and smartphones and tablets are segmented into running iOS, Android, and Windows operating systems. Also, IT managers must support multiple versions of each of these individual operating systems. Most notably, while Microsoft saw rapid adoption of its Windows 10 operating system, less than 40 percent of desktop users are currently running it. A slightly greater number of desktop users still utilize Windows 7 and Windows 8 editions, and a stunning 16 percent are still reliant on the antiquated and unsupported Windows XP platform.

Traditionally, different types of endpoints have been supported independently by different management solutions. For example, one platform might be utilized to support desktops and laptops (PCs and Macs) while another may be used to support mobile devices. Unfortunately, this approach is no longer sustainable because the lines defining endpoints are starting to blur. A casual observer, for instance, will find a large tablet with a keyboard almost indistinguishable from a small laptop. From an IT management perspective, the only difference between the two is the installed operating system, but even that is no longer a reliable differentiator. With the introduction of Windows 10, Microsoft unified its operating system to operate across all supported form factors. Similarly, for the past few years Apple has been sharing code between iOS and macOS. As a result, there are few discernable differences between smartphones, tablets, Macs and PCs. Today, there can only be one all-encompassing classification for end-user computing devices: endpoints. Today’s dynamic users require the freedom to select and move between any devices they choose without experiencing different and disjointed work environments that result from adopting disparate endpoint management solutions.

The Rising Need for Endpoint Management in a Multi-Device World

Radical changes in requirements for endpoint management can trace their origins directly to increased business needs for supporting more mobile and agile workforces. Today, according to EMA research, half of all business tasks are performed outside of a physical office building. Increased telecommuting is certainly a key factor in the expanded remote work activities, but so too is an accelerating need for users to perform tasks on the go. In either case, the productivity improvements gained from being able to immediately respond to customer requests and complete other on-demand job tasks cannot be understated.

There are, in fact, two faces of mobility that are necessary for IT to support today’s remotely-operating workforces. The first is an improvement in the portability of physical devices. Pocket-sized smartphones, tablets, and laptops can be conveniently carried and used at any location and at any time. Of course, the downside to expanded device miniaturization and
Portability is an increased chance of devices being lost or stolen, and incidents of portable device loss have kept pace with their increased adoption and use. Of equal importance to device portability is the accessibility of enterprise IT resources, such as applications, data, email, and other IT services. A good example of this would be telecommuters who access business IT resources from their home desktops. While these users are not utilizing a “mobile device,” the access to the enterprise data and applications is remote, and hence can be considered mobile. Workers have broadly embraced both aspects of mobility to the point that they are now demanding unprecedented access to business resources from any device at any location at any time.

Further increasing management complexity is the fact that endpoints are no longer necessarily purchased and owned by businesses. In fact, many organizations have introduced “bring your own device” (BYOD) programs to allow and even incentivize the employee use of personally owned devices as a means of reducing operational costs. 70 percent of mobile device users and 35 percent of laptop users reported in an EMA survey that they personally own the devices they use to perform job tasks (figure 2). This becomes a particular issue with terminated employees who used personally-owned device that contains company data, applications, and access to business systems that must be reclaimed or disabled following their departure.

Perhaps an even greater challenge derived from the consumerization of IT is that workers broadly use their devices to perform both business and non-business tasks. Specifically, according to EMA research, 91 percent of mobile devices and 77 percent of desktop and laptops that are used to perform job tasks are also employed for personal use. This problem is not just limited to employee-owned devices, but also extends to the vast majority of company-owned devices that are permitted to be used for non-business purposes. Except in the most security-conscious of organizations, asking employees to carry redundant devices or to refrain from personal employment of devices would do more harm than good. Instead, organizations must ensure enterprise policies and security requirements are met without limiting or impacting users’ personal use of their devices.
Today’s end-users have exceptionally high expectations for the availability of business IT services accessed from their devices. Further, users expect to be able to access applications and data without having to contact a help desk. Unlike past generations, today’s workers are much more technology-oriented and require little, if any, handholding. In particular, today’s users expect to have the ability to provision their own devices—a self-service experience they learned to love from accessing app stores on their mobile devices.

All of these accelerating user support requirements are conspiring with evolving IT infrastructure challenges to greatly accelerate pressures on IT managers. Unlike with traditional client/server environments, today’s more complex IT ecosystems are distributed across a variety of local and remote hosting environments, including private and public clouds, and applications are not just limited to downloadable software, but also software as a service (SaaS) applications, HTML applications, and virtual applications. Ensuring each of these elements meets established regulatory, SLA, and business requirements is challenging under the best of conditions. The ability to continuously meet enterprise security requirements is particularly difficult in these environments.

![](image)

Figure 3: Top 10 Challenges to Supporting End-user Productivity as Reported by IT Managers (by percent of respondents)

It certainly does not help that end-users are rarely very security-minded. In fact, users will often bypass enterprise security requirements if it means they are able to complete job tasks more quickly and easily. As an example, in an EMA survey of business IT users, 40 percent of respondents admitted to utilizing a public email system (i.e., Gmail, Yahoo mail, etc.) to distribute business files even though more secure email and data sharing resources were provided to them by their company. A large part of the problem is the overreliance on username and password entry as the primary method of authenticating user access. The need to constantly remember and maintain passwords
is a burden on end-users that inhibits their productivity. As a consequence, users often choose simple passwords, enter the same one for multiple accounts, and rarely, if ever, change them. Additionally, traditional signature-based malware protection solutions, which were the cornerstone of endpoint security a decade ago, can no longer be considered reliably effective, as they will not protect against “zero day attacks” that occur before the solution provider has a chance to create the signatures files and all endpoints have been updated with the new security information.

Unfortunately, many organizations still principally rely on multiple legacy endpoint management point solutions that each only addresses a particular set of endpoint devices or requirements. For instance, organizations may rely on a configuration management platform to support Macs and PCs, a mobile device management platform to support smartphones and tablets, and an endpoint security platform to help ensure compliance attainment. Interacting with multiple independent solutions results in inefficient “swivel-chair management” that requires administrators to perform duplicate tasks on each solution’s interface. In addition to wasting valuable time on mundane tasks, using independent platforms make it nearly impossible to correlate events and management conditions in order to perform root cause analysis and establish common administrative practices. Since the solutions are typically offered by different vendors, they can also be extremely costly to maintain due to the need for multiple sets of licenses and maintenance contracts.

Empowering Users with Unified Endpoint Management

Addressing today’s evolving challenges for meeting end-user computing requirements, delivering IT services from distributed hosting environments, and meeting security commitments requires a fundamental shift in management practices and solutions. Rather than utilizing separate solutions for provisioning, securing, and supporting heterogeneous end-user devices, a unified endpoint management solution integrates and consolidates the various administrative tasks into a common set of management processes all accessed from a single “pane of glass.” This approach is broadly recognized as the most effective solution to combatting increased complexities in end-user computing. In fact, when EMA surveyed IT managers responsible for supporting end-user requirements in their organizations, 75 percent of respondents indicated they believe the ability to manage multiple device architectures in a consistent manner is important to their overall business performance.

There is a common misconception that UEM simply extends traditional end-to-end client lifecycle management processes for supporting PCs and Macs to also support mobile devices. This is inaccurate on many levels. End-to-end control over endpoints is only practical when principally supporting a single architecture (such as Windows desktops). Applying this same approach to a wide range of different device types is tantamount to attempting to drink the ocean. Full endpoint configuration management was actually attempted shortly after mobile devices started appearing in workplaces with the introduction of mobile device management (MDM) solutions that emulated laptop management concepts on smartphones and tablets. However, adopting organizations quickly recognized they did not actually require many of the complex and ultimately unnecessary processes. As a result, mobile management practices moved past MDM to enable enterprise mobility management (EMM) solutions that focus on the secure delivery of applications, data, and services to mobile endpoints, rather than end-to-end control of the devices.
The lessons learned from the evolution of mobile management can also be applied to desktop and laptop management. While some device management capabilities—such as patching, updating, and malware protection—are still more efficient and effective to perform centrally, the majority of endpoint control should be in the hands of the users. This allows them to customize the experience in the ways most applicable to their unique work style. The primary role for IT administrators, therefore, is to ensure software and other digital services are continuously and securely accessible regardless of the devices from which users are accessing them. Identified below are the essential characteristics that must be included in any UEM solution:

- **Centralized Application Management** – All application types (such as ipa, apk, pkg, dmg, appx, msi, and exe files) should be identified, stored, distributed, and reported from a single unified platform. Common processes should be adopted that support and secure applications on all public and private hosting environments. Policies defining software access, use, and configurations should also be centrally defined. Application distribution and installation tasks should now be consolidated into a single automated process.

- **User Self-Service** – End-users should have the ability to enroll their own devices into the management service. Users should also have the ability to turn optional features on and off, such as location tracking of their devices. Applications, data, and other IT services should be made accessible from an enterprise app store, emulating the same convenience users experience with public iOS and Android app stores on their mobile devices.

- **User Experience Management** – Applications, data, email, and other IT services must be easy to access and use with processes that are intuitive, fast, and reliable. Users should not have to “jump through hoops” to access business resources necessary for them to perform job tasks, regardless of where they are located or what device they are using. To enhance user productivity, rather than inhibiting it, authentication tasks (i.e., entering passwords, PINs, VPN connections, etc.) should be minimized, and organizations should utilize single sign-on (SSO) capabilities for all accessed business IT services. Non-password forms of authentication, such as biometrics, behavioral analysis, and device authentication should also be employed whenever possible.

- **Resources Isolation** – To support BYOD initiatives and allow non-business uses of endpoints, applications and data on user devices should be logically segmented into business and personal categories. Common solutions adopted to achieve this include containerization and app wrapping. In the event an employee should be terminated or their device should be lost, stolen, or otherwise compromised, business-related services can be selectively locked or wiped to prevent unauthorized access without affecting a user’s personal software resources.

- **Enhanced Security** – All supported devices should be continuously monitored for suspicious activity in real-time. Any devices determined not to be in compliance with business requirements should be immediately remediated or prevented from accessing and using business resources. All managed endpoint devices should also be continuously updated with the latest security patches. Patch management and distribution should be administered centrally and include package staging locations, rather than direct connections to service providers, in order to minimize impacts on wide-area networks. Additionally, secure methods for data sharing and email must be provided to end-users that are easy to use to ensure they will be inclined to use them.
• **Cognitive Analytics** – Data collected on device, software, and user states and conditions increases proportionally with the number of supported endpoints. This excessive information can overwhelm administrators with mostly irrelevant status reports, causing them to ignore potentially critical messages. Analytics should be used to sift through all the “white noise” of collected data to identify relevant information that will provide actionable insights for improved management and control.

• **Reporting and Alarming** – Security states and the performance status of all supported endpoint devices should be continuously monitored. Analytics should be applied to collected data to identify any potential security threats or service-impacting issues. Any identified issues should be automatically remediated or promptly brought to the attention of IT administrators. Custom reports on endpoint states should be able to be generated on-demand to provide proof on compliance and intelligence on service performance and improvement opportunities.

**Enabling Effective Unified Endpoint Management**

While most IT managers recognize that traditional endpoint configuration management practices are no longer sustainable in today’s multi-device, hybrid-cloud, and security-conscious IT ecosystems, they are challenged with transitioning their environments to a more effective approach. Often IT managers feel they must make the impossible choice of supporting business requirements for security and user support or achieving goals for reducing operational costs and efforts. Paralyzed due to budget constraints and limited resources, IT managers often opt to only officially provide limited endpoint support, commonly just for Windows devices, leaving employees to fend for themselves with supporting non-Windows platforms. Not only does this reduce workforce effectiveness—it places the business at significant risk of security breaches.

Organizations should not have to choose between meeting business requirements and budget constraints, and a pragmatic approach to UEM allows them to have their proverbial cake and eat it too. Consolidating management processes into a single solution focused on IT service delivery, rather than endpoint configuration and control, has a profound impact on reducing costs and minimizing administrative efforts while improving service reliability and end-user satisfaction. This is because administrators utilize a common set of processes and tools to perform a strategic set of tasks targeted at enabling end-user productivity and are no longer overwhelmed with performing mundane tasks such as application deployments.

The key to success in enabling a responsible approach to UEM is adopting an automated management platform that integrates essential capabilities for administration, provisioning, and security, accessed from a single console interface and governing all endpoints supported by the organization. Ease of use with the platform is critical to minimize administration efforts and enable rapid responses to end-user requirements. User access permissions and application configurations should all be governed by policy-based profiles, so administrators do not need to be involved in day-to-day mundane provisioning tasks. Ideally, the solution will be integrated with listing services (such as Active Directory) to enable consolidated, pre-defined group management of policies. Also, policies should be aware of the end-user context so they can automatically adjust to particular use cases. For instance, a more stringent security policy may be necessary for users accessing business servers from remote locations, rather than from within business workplaces or over business networks.
By empowering end-users with the freedom to configure and manage their own devices, administrators are able to focus on introducing new IT improvements and business services. The introduction of an application portal is central to end-user empowerment, but it must aggregate access to all software types and hosting locations, including SaaS applications, web applications, and virtual applications. Additionally, a pragmatic UEM platform which monitors application performance and software usage patterns can ensure purchased application licenses are actually being used and to reclaim and repurpose those that are not. Efforts and related costs for achieving security assurance and regulatory compliance achievement are also greatly reduced with a UEM platform that consolidates security vulnerability assessments for all devices in real-time to continuously identify both known and unknown threats before they become business-impacting.

As an example of a responsible approach to UEM, the IBM® MaaS360® with Watson™ platform offers a consolidated solution for supporting heterogeneous endpoints (including Windows XP, 7/8/10, macOS, iOS, Android, and IoT devices), all from a single, centralized console. The solution is hosted on IBM’s own public cloud, licensed by subscriptions, and requires no additional hardware, software, or maintenance investments. Endpoints are automatically detected, identified, and enrolled in the solution with little to no administrator interaction. Once enrolled, user access is enabled and governed by pre-built, policy-based user profiles that automatically ensure compliance with business requirements. BYOD programs are supported by logically isolating business resources from personal resources on endpoints, and patching processes are greatly simplified on PCs and Macs with automatic target identification and centrally distributed deployments that also minimize network impacts and ensure updates are successful. Additionally, MaaS360’s direct integration with the IBM Watson platform delivers cognitive insights, contextual analytics and cloud-sourced benchmarking capabilities that enhance support of endpoint devices, applications, data, and IT services with real-time security protection, risk analysis, service improvement opportunities, and general insights on endpoint management states.

Figure 4: IBM MaaS360 with Watson Advisor for Cognitive Unified Endpoint Management
EMA Perspective

UEM fundamentally alters the way administrators support end-user computing requirements and the way users interact with business technology. The advantages of this approach can be summed up in three key areas. The first, and arguably most important, is the seamless enablement of security assurance. An EMA survey of IT managers identified that ensuring network and data security was the endpoint management practice most important to their business, the most difficult to perform, and the most time-consuming to complete. A unified endpoint management approach not only reduces security enablement efforts but also provides organization with the confidence that all supported devices and IT services are continuously secured and risks to the business are minimized regardless of the type of devices accessing business resources and where they are located.

The second key advantage to UEM is its potential for simplifying overall endpoint administration practices. Traditional end-to-end configuration management processes were challenging enough for IT administrators when managing a single platform (i.e., Windows PCs). Now tasked with supporting an increased number of heterogeneous devices in complex IT ecosystems, IT administrators are becoming frustrated with having to satisfy the expanding number of mundane user requests. At the same time, more technology-savvy workforces are becoming less tolerant with having to rely on administrators in order to configure and use their devices. UEM centralizes support for all devices, substantially reducing the number of steps administrators need to perform, while transitioning some maintenance tasks into the control of the end-users. This frees up administrators to focus on optimizing the secure delivery of IT services and on introducing new business-focused services. Additionally, consolidated support responsibility simplifies organizational structures. Rather than having separate teams support PCs, Macs, mobile devices, their security in addition to siloed IT services, UEM allows a single support department to administer all devices in a consistent manner.

A further benefit from reducing management efforts is the reduction of related costs. In fact, 45% of surveyed organizations indicated to EMA that they had achieved quantifiable management cost saving solely from the adoption of automated solutions designed to support BYOD requirements.¹

While the first two value propositions to adopting a UEM platform are most frequently cited by IT managers, organizations should also recognize the immense advantages achieved from empowering their workforces. UEM grants users the freedom to utilize the devices they wish to use, choose when and where they wish to use them, and select the applications that will make them most productive. This also boosts user experiences and job satisfaction rates, helping to retain valuable workers. Empowered workforces are more productive and have greater agility for meeting rapidly-changing business and market requirements. This translates into improved revenue opportunities and an accelerated ability to meet organizational goals and objectives.

The key to realizing the value from a UEM approach is the adoption of a fully integrated platform that is both comprehensive in its support of multi-device endpoint requirements and its ease of use. The solution must enable the administration of all supported endpoint devices in a consistent manner from a single console interface. A comprehensive platform, such as IBM MaaS360 with Watson, will deliver the reliable automation for policy-based endpoint management that enables organizations to responsibly regain control over their distributed end-user computing support stacks.

¹ Effective BYOD Management: Empowering a Mobile Workforce, 2016
About IBM Security
IBM offers advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit [www.ibm.com/security](http://www.ibm.com/security), follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA’s clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at [www.enterprisemanagement.com](http://www.enterprisemanagement.com) or [blogs.enterprisemanagement.com](http://blogs.enterprisemanagement.com). You can also follow EMA on Twitter, Facebook, or LinkedIn.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2018 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.