Survival Guide to Multi-Device Support in the Age of Mobility

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper and Case Study
Prepared for Ivanti

April 2017

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Survival Guide to Multi-Device Support in the Age of Mobility

Table of Contents

Executive Summary 1

The Evolution of Endpoint Management 1

Emerging Requirements for Multi-Device Support 3

- Rising Number of Devices Per User 3
- The Consumerization of IT 3
- Escalating User Expectations 3
- Expanding Business Risks 4

Multi-Device Support Survival Guide 5

- Simplifying Management 5
- Managing OS Migrations 5
- Isolating Business Resources 6
- Creating Consistent User Experiences 6
- Ensuring Security without Compromising Productivity 6
- Improving Business Efficiency 7

EMA Perspective 8

About Ivanti 8

Executive Summary

Increased reliance on workforce mobility has resulted in a dramatic increase in the number of endpoint device platforms requiring support in modern business environments. Challenged to provision and secure multi-device support stacks while ensuring productive and satisfying user experiences, organizations must adopt consolidated management practices and administrative tools. Enabling unified support of smartphones, tablets, laptops, and desktops from a single console necessitates a fundamental change in the approach to endpoint management. Rather than focusing on the end-to-end control of user devices, organizations must target efforts on the secure delivery of enterprise applications, data, and services.

The Evolution of Endpoint Management

Welcome to the age of mobility. It's an era punctuated by an unprecedented level of user productivity, increased freedom to employ preferred applications, and unfettered remote access to critical enterprise data—at least that's how it has been advertised. When executed properly, enterprise mobility management (EMM) processes and solutions can indeed deliver on the promise of increased workforce performance and accelerated business agility. However, there is much that needs to be accomplished behind the scenes to enable the seamless and secure delivery of enterprise IT resources to remote PCs and mobile devices.

To fully appreciate the complexity of enterprise challenges to supporting a mobile workforce, it is necessary to review how endpoint management requirements have evolved to their current state. The cornerstone of enterprise user computing has traditionally been the PC, and in most organizations this principally required support for a single operating environment—Microsoft Windows. While a few Mac and Linux PCs may have been deployed in some organizations, Windows has consistently dominated more than 90% of the enterprise PC market. This has allowed for a standardization of processes for client lifecycle management that delivered end-to-end device administration and control. With only a single architecture to worry about, IT operations teams were able to employ automation tools to maintain comprehensive security and optimized performance across the support stack. However, the value of this targeted approach began to diminish with the introduction of smartphone devices into the workplace. Of particular note were personally owned iOS and Android devices purchased and brought into the workplace by employees. This trend continues to this day as the "consumerization of IT" continues to ensure that vendors focus development and marketing of devices on personal users rather than directly to businesses, and it has expanded to impact the production of tablets and laptops as well.

With the influx of mobile devices into the workplace, organizations were suddenly required to expand endpoint management practices to support a much broader range of operating environments. Initial automation solution suites for mobile device management (MDM) were primarily security-focused point solutions that lacked any integration with traditional PC management tools. For some time, this dual management experience—one solution to support PC and a separate solution to support mobile devices—was the accepted norm for endpoint management. However, trends in PC development are blurring the lines between what is a PC and what is a mobile device. Size is no longer the defining factor of the two as larger tablets may now be much bigger than small laptops, and convertible devices are creating dual user experiences as they are able to be used sometimes as a tablet and sometimes as a laptop. Even more significant is the fact that the operating systems of the two environments are merging. With the release of Windows 10, Microsoft has unified its operating system across all user

As the hardware and software architectures converge, it is no longer sustainable to support devices with two completely independent sets of management practices and automation tools.

devices. Additionally, Apple is now sharing code between MacOS X and iOS, and Google has enabled its Chrome OS to run Android applications. As the hardware and software architectures converge, it is no longer sustainable to support devices with two completely independent sets of management practices and automation tools.

Unified endpoint management (UEM) has emerged to deliver governing solutions for managing and securing all smartphones, tablets, laptops, and desktops from a single administrative console. The approach reconciles discrepancies between enterprise mobility management (EMM)—which incorporates MDM with mobile content management (MCM) and mobile application management (MAM)—and PC lifecycle management—which includes solutions for PC device, data, and application management. Management solutions that adopt a UEM approach employ a centralized management console, a common reporting engine, and a unified asset database to support all endpoint devices in the support stack. Ideally, a UEM solution will enable the creation of a single user profile to govern authorization, configuration, and security policies for all devices employed by a user to perform business tasks. The goal of UEM is to deliver a seamless management experience for all supported user devices that is easy to administer and still meets the most stringent security requirements.

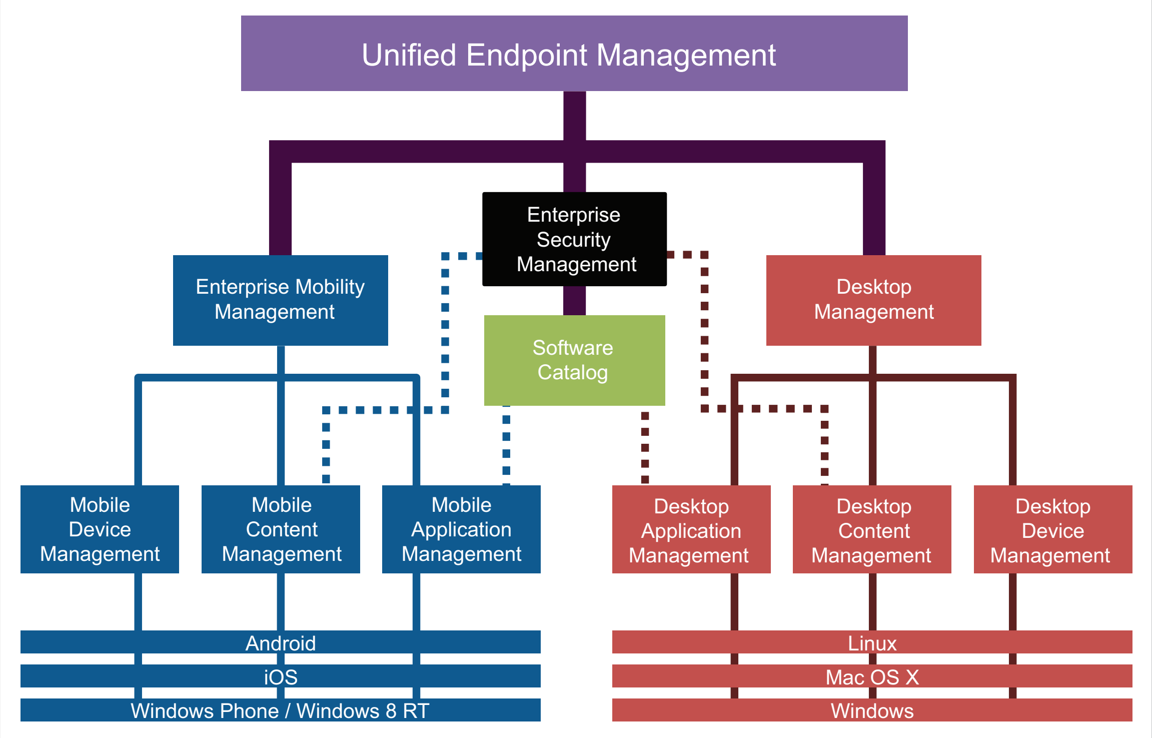
Unified Endpoint Management
Enterprise Security Management
Enterprise Mobility Management
Software Catalog
Desktop Management
Mobile Device Management
Mobile Content Management
Mobile Application Management
Desktop Application Management
Desktop Content Management
Desktop Device Management
Android
iOS
Windows Phone / Windows 8 RT
Linux
Mac OS X
Windows

Figure 1: Diagram of a Unified Endpoint Management architecture

Emerging Requirements for Multi-Device Support

Rising Number of Devices Per User

While today's discussions on endpoint management requirements principally focus on the support of mobile devices (i.e., smartphones and tablets), it is a mistake to believe this in any way diminishes the role PCs continue to play in the modern enterprise. According to EMA primary research, 98% of business users regularly use a Windows or Mac desktop or laptop PC as part of their job function, and 87% rely on both a PC and one or more mobile device. Clearly, mobile devices are being adopted to supplement PCs rather than to replace them. As a result, organizations must support an exponential increase in the number of devices in their support stacks as well as a much broader range of hardware and software platforms. This problem is further exacerbated by the current trend in adopting wearable devices, such as smartwatches, smart bracelets, smart glasses, smart rings, and smart clothing. These devices are commonly tethered to a smartphone or tablet via a Bluetooth connection over which sensitive enterprise data may be sent (in the form of a message or an email), creating a substantial security risk if the device is lost or the transmission is intercepted.

The Consumerization of IT

Compounding the challenges of the management of endpoint devices, the consumerization of IT has had a direct impact on how business IT resources are delivered, managed, and secured. More than half of all mobile devices and a quarter of all PCs that are used to perform business tasks are employee-owned. Regardless of who owns the devices, though, it is actually more important to recognize that 90% of mobile devices and 77% of laptops are used to perform both business and personal tasks. For mobile devices, this has prompted the introduction of "bring your own device" (BYOD) management practices that ensure the delivery and security of business applications and data without limiting an employee's ability to use their devices for personal enjoyment. However, similar BYOD practices have not yet substantially been introduced for PC platforms—though the need for this is increasingly being acknowledged.

Escalating User Expectations

Expanded user expectations are further increasing pressures on enterprise IT operations. On-demand and self-service capabilities are common in consumer-focused mobile applications, and users are now demanding that same responsiveness in the delivery of enterprise software and services. Access to applications, data shares, email, remote access portals, and any other business resources must be quick and easy to perform, reliable, and highly available. Also, user experiences in accessing business resources must be intuitive and consistent across all the devices they employ. However, creating intuitive user experiences has also become a challenging process. Unlike traditional environments that store all applications and data on centralized enterprise servers, modern organizations rely on resources that are distributed across complex internal and external ecosystems. Applications may be local static apps, virtual apps, cloud apps, streamed apps, or web apps, and data may be stored in public or private data shares or SharePoints. IT organizations must deliver these distributed resources to end users securely while still meeting the increased expectations for a simplified user experience. The process is akin to pulling off a magic trick—the audience must not see how the rabbit got into the hat in the hope that they will be amazed when the rabbit is pulled out of the hat.

Expanding Business Risks

Mitigating security risks in a way that does not diminish user experiences is particularly challenging because of the impacts of workforce mobility. Physical devices containing sensitive data are easily lost or stolen, terminated users may continue to retain access to privileged information on personal devices, and the inadvertent contraction of malware (viruses, spyware, Trojan Horses, etc.) from an increasing number of public sources is on the rise. Arguably of even greater concern today is the proliferation of poor data sharing practices on remote laptops and mobile devices. According to EMA survey-based research, 89% of business professionals rely on unsecured email as their principal means of sharing business data. While this is a quick and easy method of transferring data, it is easily one of the highest risk factors in enterprise security since it has the potential to take critical business data completely outside the control of the company. This exemplifies the need for introducing security practices that work in parallel with enhancing user experiences. If users are challenged to do their job, they will resort to unsecure and non-approved methods to complete their tasks. They may even bypass enterprise security altogether by rooting or jailbreaking their devices. With all these factors in play, IT operations must enable holistic visibility across all supported devices to achieve prompt remediation to security risks.

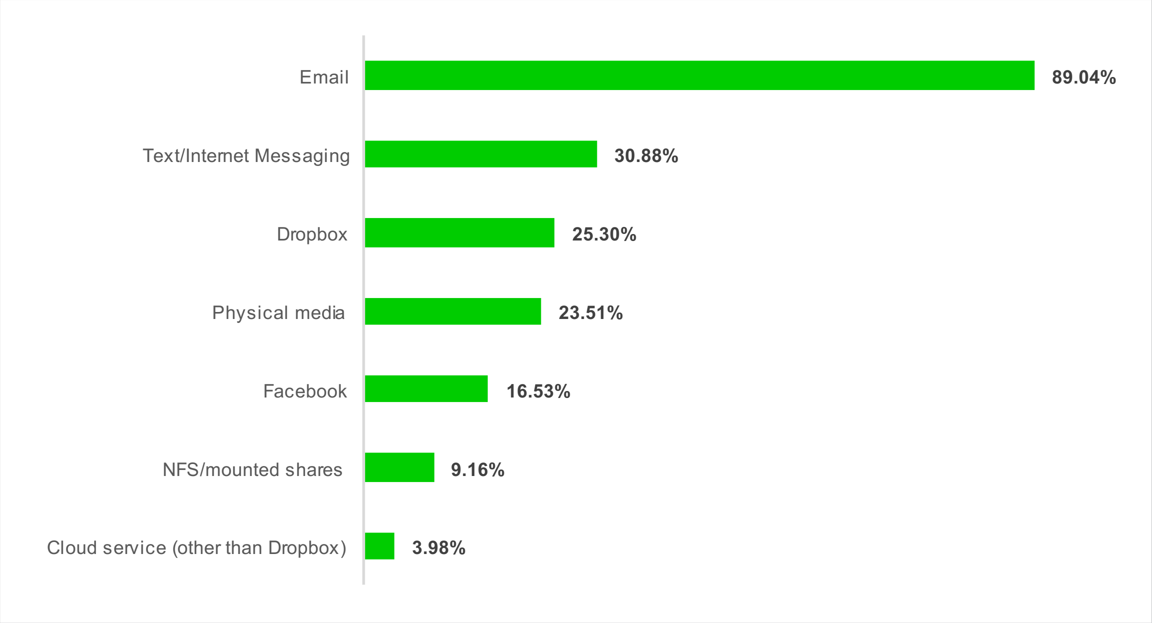

Figure 2: Percent of survey respondents indicating unsecured data sharing methods they regularly use to perform job tasks

Multi-Device Support Survival Guide

Identified below are the management elements essential for responding to emerging requirements for multi-device support in the age of mobility. While individual organizations may need to customize the solutions to meet unique business conditions and requirements, the most effective approaches always involve a combined adoption of process improvement and comprehensive automated management solutions.

Simplifying Management

The key to reducing administrative efforts is employing a common management platform that supports all endpoint devices in a support stack. In addition to traditional Windows PCs, this means enabling unified management for an increasing number of Macs as well as all supported mobile device platforms (most notably iOS, Android, and Windows Mobile) from a single dashboard. Organizations should begin by collecting comprehensive hardware and software asset information (including device configurations, installed applications, license details, and compliance status with security requirements) on supported devices and store the information in a single centralized data repository. This information can then be mined to provide holistic reporting and dash-boarding on the status of all devices from a single console, enabling administrators to rapidly identify issues and initiate remediation steps. Utilizing a common interface for establishing policies and user profiles for all devices will also reduce management efforts by eliminating the need for "swivel chair management" and simplifying processes for event correlation, root-cause analysis, and compliance auditing.

Even with a UEM platform in place, most organizations will find the end-to-end control and management of an increasingly heterogeneous support stack to be unsustainable. Instead, IT operations should focus efforts on the secure delivery of IT resources (e.g., applications, data, email, etc.). Limit administration practices on endpoint devices to just those that are essential to ensure they are able to reliable access and run enterprise IT services and can meet established security requirements. This should include rooting and jailbreaking detection, enterprise network configuration, malware protection, and the distribution of containers or other dedicated workspace environments. For any other device management activities—such as software provisioning and OS updating— the user should also have the option to self-serve in addition to IT carrying out the rollout.

Managing OS Migrations

As users are granted greater freedom to select from a variety of device platforms, administrators will need to enable secure and reliable methods for rapidly transitioning user environments. For instance, there is an increased interest in business users planning to migrate to Windows 10, or to transition from Windows PCs to Mac PCs, and it is not uncommon for users to change mobile device platforms every three years when their provider contracts expire. To minimize the impact of migrations on end user productivity, transition processes must ensure preexisting user environments are replicated in newly installed environments. Before initiating an OS migration, record details must be collected on the applications the user employs as well as the configuration of system, desktop, and application settings. These user-specific elements can then be mapped to the new environment (i.e., post-migration) to ensure a consistent user experience. User-centric, policy-based deployment of apps, content and configurations across operating systems more easily enables this process, by setting conditions based on user role first, device type and operating system second.

Isolating Business Resources

Organizations supporting BYOD clients or, in fact, any environment where users are permitted to employ their devices for non-business purposes must isolate enterprise applications and data to ensure their access and use does not violated established security requirements without impacting the users' personal enjoyment of the devices. Methods for accomplishing this include containerization (accomplished either via a full container or native hardware/OS APIs), app wrapping, virtualization, and the deployment of enterprise-dedicated applications. Regardless of the method employed, management of the isolated business resources should be performed from a centralized interface that utilizes configurable profiles to identify specific levels of access and usage restrictions for each mobile user.

Creating Consistent User Experiences

Success in any endpoint management approach can be gauged by the level of user satisfaction achieved. The better an experience a user has with accessing business resources from their devices, the greater will be their productivity and job performance. Users must be able to access applications and perform tasks in the same manner regardless of the device they happen to be using. Establishing a consistent user experience requires the introduction of standardized user self-service processes. This can take the form of a user portal, software catalog, or enterprise app store. Access privileges and security restrictions should be defined in a common set of customizable user profiles. To ensure consistency across endpoint device platforms, user profiles should leverage group and user information in an enterprise listing service (such as Active Directory). Policies can then be applied to these predefined groups or user roles that are standardized for each supported endpoint platform.

Success in any endpoint management approach can be gauged by the level of user satisfaction achieved.

A standardized workspace should also be provided that presents a consistent desktop look and feel across supported devices. Ideally, this workspace will operate independent of a user's non-business applications and data to support BYOD requirements. Technologies that support this include containerization, desktop virtualization, and web-hosted aggregated workspaces.

Ensuring Security without Compromising Productivity

While enterprise security and compliance requirements must be maintained on any device that accesses business applications and data, risk mitigation processes should be nearly invisible to end users so as not to diminish their productivity or work experiences. Essential to this achievement is the introduction of a secure data-sharing service (such as a secure FTP site, an enterprise SharePoint, or a compliant cloud-storage environment) that is only accessible by authorized personnel via enterprise-controlled access points. Other data loss prevention tactics include restricting cut and paste of business data, isolating business resources, and restricting remote access of devices to internal business servers. Data encryption should also be employed whenever possible so that even if sensitive files are somehow released externally, they will still not be useful to unauthorized individuals.

Centralized reporting and automated remediation of security configurations should be enabled for all devices to ensure endpoints do not drift out of compliance with regulatory or corporate policies. This requires the development of a standardized set of security profiles to govern each device type and unique user requirements. For instance, it may be necessary to limit physical or network ports to prevent the unauthorized broadcast distribution of sensitive data or its duplication onto removable media. Similarly, dangerous applications may need to be blacklisted or, in higher security environment, only approved applications may be whitelisted for installation on remote devices. Where applicable, security patches should also be centrally distributed to endpoints to ensure devices are rapidly updated to the latest releases. Each of these configuration elements should be defined and controlled based on contextually aware information. That is, individual security profiles should enforce a unique set of policies depending on the endpoint state, including the type of device, user requirements, user access rights, the physical location of the device, and/or the point of network access. To meet compliance objectives and to ensure prompt risk mitigation, reporting and dashboarding of the entire multi-device security ecosystem should be provided in an easily digestible format that will intuitively direct administrators to potential breaches. Any device identified as violated an established security policy should have its access to enterprise systems and data revoked until the problem has been remediated.

Improving Business Efficiency

By its very nature, empowering a mobile workforce through unified endpoint management improves business efficiency. Ensuring users are able to perform business tasks from any device and at any location grants them the freedom to meet their job requirements in the manner in which they will be most productive. It enables them to employ the platforms, applications, and interfaces with which they are most familiar, allowing them to focus on doing their job rather than manipulating their devices. Additionally, the portability of devices frees users from the constraints of the physical workplace, enabling greater agility in their ability to respond to emergencies, customer requests, and rapidly changing business requirements. Being untethered from the business network also improves employees' job satisfaction as they have the ability to travel, telecommute, and more easily provide out-of-hours support without diminishing their productivity. All of this translates into an improved ability to meet business goals as users are able to perform a greater number of tasks and each with a greater effectiveness.

The adoption of UEM practices translates into financial benefits that can be applied to all endpoint devices. In traditional PC environments, users are provisioned with a common set of applications whether they used them or not. Self-service provisioning, however, allows users to install the applications they desire, while asset and license management solutions can be leveraged to ensure access is granted only to applications they will actually use and are entitled to use. Further, CapEx savings can be achieved by leveraging holistic endpoint intelligence that enables the adoption of less costly hardware and software resources that are determined to be sufficient to meet user requirements. For instance, a tablet may be identified as sufficient for someone not requiring the higher performance of a laptop or desktop PC. The OpEx cost of IT administration can be also reduced by focusing administration efforts on the delivery of IT services rather than on end-to-end device management. Support time and related costs can be further reduced with the adoption of automation (especially if it is automation that enables user self-service management) as this reduces the burden on the IT operations staff.

EMA Perspective

Any analysis of modern enterprise endpoint management requirements must conclude with one inescapable truth—we live in a multi-device world. Businesses that embrace the reality of broad device heterogeneity and adopt processes and solutions that directly address related challenges with a consolidated approach will undoubtedly achieve a competitive advantage over those stuck in the rut of maintaining independent, device-centric management practices. Achieving this requires a different way of looking at endpoint devices. They should no longer be segmented into arbitrary categories—such as smartphone, tablet, laptop, and desktop—but should be regarded collectively as devices used to access business applications and data.

UEM solutions provide the fundamental practices and tools to enable multi-device support that is agile, simplified, and cost-effective. Rather than trying to "drink the ocean" by extending antiquated end-to-end PC management and control practices to mobile platforms, UEM solutions seek to liberate PC endpoints by adopting lessons learned in enterprise mobility management. IT administrators should be focused on the secure and reliable delivery of business applications and data, and users should be empowered with self-service features to manage their own devices. It must also be recognized that most endpoints will also be used for non-business purposes, so business resources should be isolated to ensure their secure use when accessing business resources without limiting users' personal enjoyment of their devices. EMA recommends any business supporting a multi-device environment adopt an automated management solution that provides holistic visibility, consolidated management, and integrated security across all endpoint devices from a single unified console.

About Ivanti

Ivanti is IT *evolved*. By integrating and automating critical IT tasks, Ivanti helps IT organizations secure the digital workplace. For more than three decades, Ivanti has helped IT professionals address security threats, manage devices and optimize their user experience. From traditional PCs, to mobile devices, virtual machines and the data center, Ivanti helps discover and manage your IT assets wherever they are located, improving IT service delivery and reducing risk. Ivanti also ensures that supply chain and warehouse teams are effectively leveraging the most up-to-date technology to improve productivity throughout their operation. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

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 or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3346.040617