Unified Endpoint Management: Simplifying the Security and Support of PC and Mobile Devices

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper

Prepared for Ivanti

January 2017

Executive Summary

In order to gauge the principle challenges to and most valuable solution for achieving effective enterprise endpoint management, Enterprise Management Associates™ (EMA®) conducted principal, survey-based research on the enterprise adoption, use, and administration of desktops, laptops, tablets, and smartphones. Responses from more than one hundred IT directors knowledgeable about their organization's endpoint management operations were evaluated to identify trends. Key findings of the research include:

- Roughly half of all business professionals rely on both a PC and a mobile device to regularly perform business tasks
- Ensuring data security is considered the greatest challenge to supporting end-user productivity
- More than half of organizations supporting Apple devices (MacOS and iOS) reported at least some difficulty performing key management tasks, indicating that Apple devices are the most challenging to support
- 68% of respondents reported they were aware of a security breach that occurred within their company within the preceding 12 months
- According to one-third of respondents, security management accounts for a significant or majority of administrator time to complete, making it the most time-consuming management practice

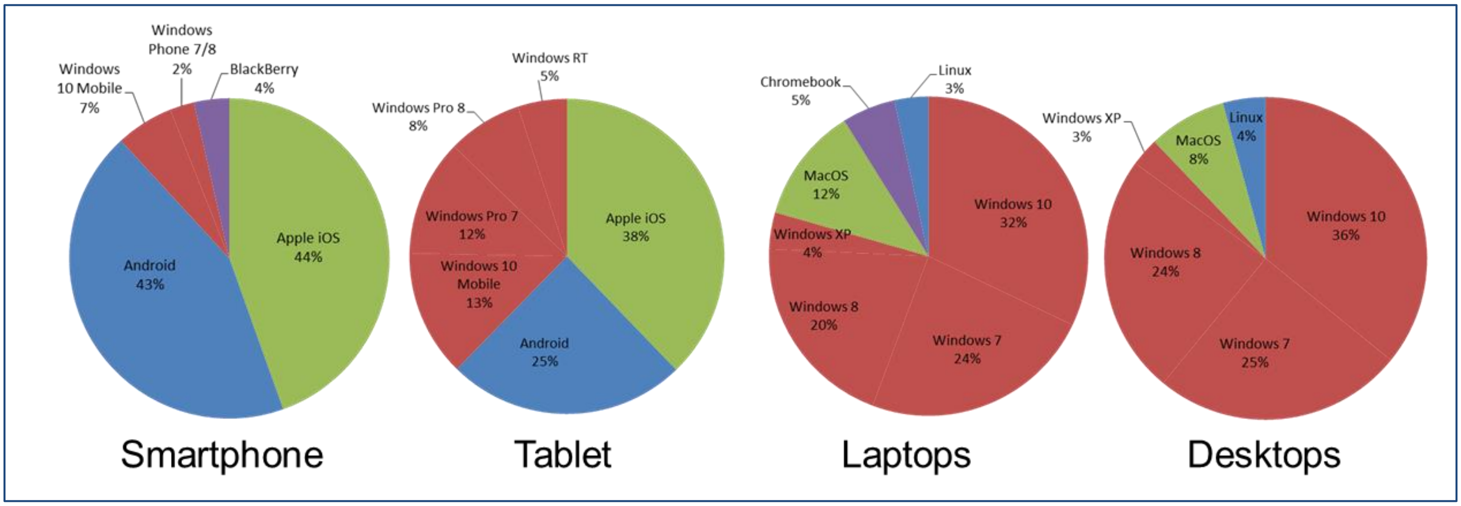
Challenges to Enabling Multi-Device Support

We live in a multi-device world. According to EMA primary research, the average business professional regularly employs at least two computing devices—including desktops, laptops, tablets, and smartphones—to perform job tasks. Moreover, roughly half of all workers utilize both a PC and a mobile device in the course of a typical day at the office. While desktop and laptop PCs continue to be the primary resources for performing job tasks, increased requirements for supporting workforce mobility has led to the broad adoption and use of mobile devices as well. In fact, roughly half of all business tasks are now performed outside a physical workplace and beyond the control of secured networks. All of these factors conspire together to radically increase the burden of endpoint management requirements on IT support professionals.

Noted below are key findings from EMA's survey-based research, identifying requirements for multi-device support.

Device Adoption

Less than a decade ago, organizations principally standardized endpoint environments on a single platform: Windows. Since then, the extensive adoption and use of mobile devices has not only exponentially increased the number of physical endpoints that need to be supported; it also broadened the number of operating systems that must be secured and managed. While Apple iOS and Android devices have consistently dominated the mobile market, Microsoft Windows has recently gained significant growth in the enterprise tablet market (Figure 1). Much of this success can be attributed the introduction of Windows 10, which was architected to unify the operating system across all endpoint devices, allowing common applications to be used on different devices without any rebuilding or recompiling. EMA market trending analysis indicates Windows 10 tablet adoption is directly stealing market share from Android devices and is frequently employed by organizations that are purchasing tablets for their workers. While Windows 10 adoption has also been very aggressive in the PC market, the enterprise use of Macs has also increased (doubling since 2015), and the introduction of Chromebooks to many workplaces has only served to further increase endpoint heterogeneity.



Smartphone Tablet Laptops Desktops

Figure 1: Multi-platform adoption

Management Challenges

A typical IT support organization must today support a minimum of four different operating environments, each with unique configurations, applications, services, and security protocols. According to surveyed IT managers, the need to support multi-device architectures ranks among the top three challenges in supporting user productivity (Figure 2). Further, the other two leading challenges (ensuring data security and reducing IT management costs) are directly related to multi-device support requirements. Achieving security is difficult because each device architecture has its own set of constantly-changing vulnerabilities. Protecting business applications and data requires monitoring, authentication, encryption, resource isolation, and patching solutions all tailored to meet the exacting requirements of the endpoint devices from which they are being accessed. Similarly, the cost of IT management increases proportional to the number of device architectures in the support stack, as each requires dedicated tools and administrators specifically trained on their use.

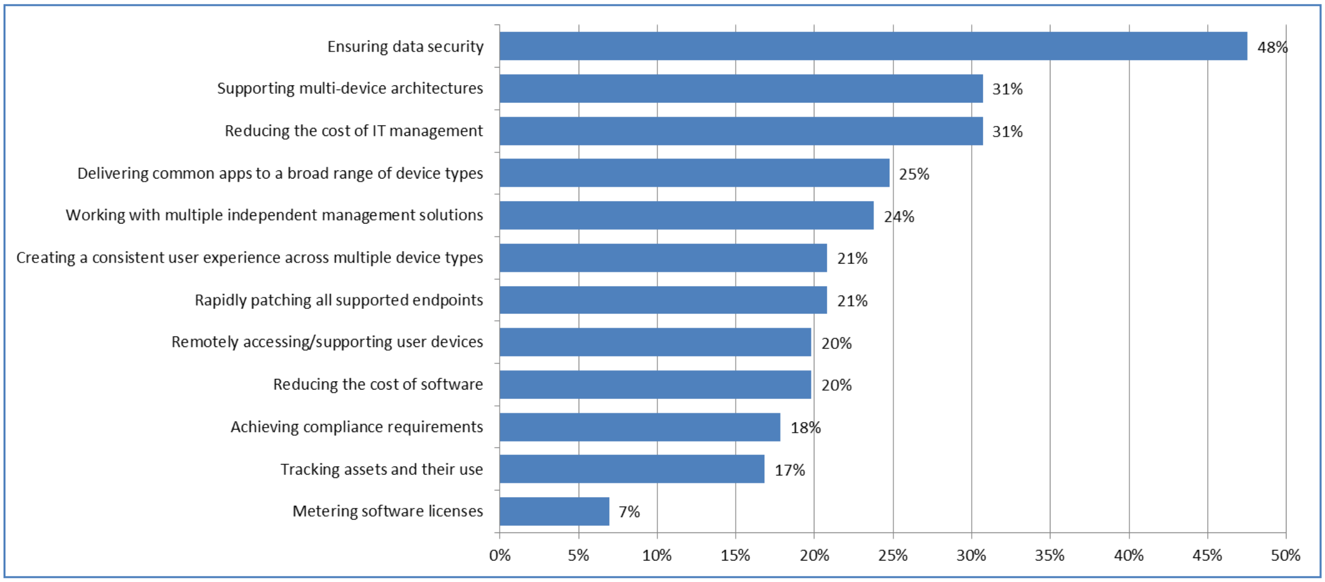


Figure 2: Greatest challenges in supporting end-user productivity

Apple Management

As organizations increasingly adopt Apple devices to accommodate user preferences and evolving business requirements, the importance placed on support for Apple devices is growing proportionally. 24% of survey respondents from organizations that manage Apple devices indicated support for MacOS and iOS platforms was “very critical” to their business success. However, respondents also indicated that that number can be expected to rise to 41% within the next two years. This implies an expanding IT management challenge is evolving since organizations supporting Apple devices reported a greater-than-average difficulty in performing related management practices. This is indicative of the fact that MacOS and iOS platforms require specialized support resources that are not commonly included in management solutions that were principally designed to support Windows architectures. In fact, more than half of organizations that support Apple devices reported at least some difficulty with performing key Apple-focused management tasks (Figure 3). Of particular note were processes for predefining configuration for the Apple Device Enrollment Program, as well as deploying applications and patches to MacOS endpoints.

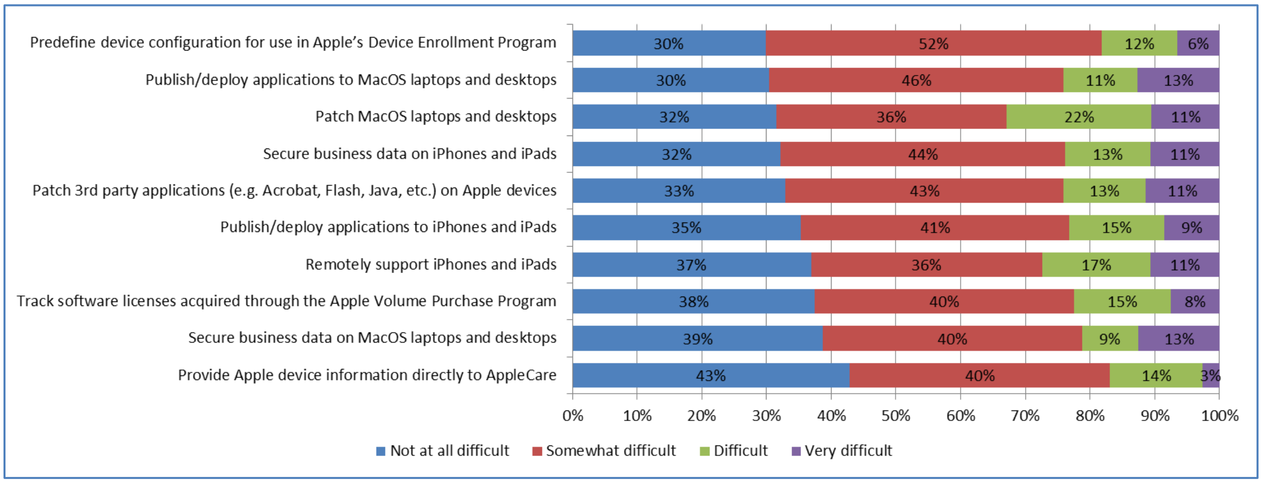


Figure 3: Difficulty in supporting Apple management tasks

Comparing MacOS adoption rates with EMA research results from one year prior indicates the business use of Apple laptops and desktops has increased by roughly 40% in that timeframe. Additionally, iPhones and iPads continue to dominate the enterprise mobile management market. There is no indication that these trends are slowing down, so organization are increasing being pressured to provide more extensible support for Apple devices.

Endpoint Security

Security was repeatedly noted as a primary focus for IT managers across EMA’s survey results. In addition to being the most challenging to support, security was identified as the most time-consuming, the most difficult, and the most costly administration practice. Even with all this attention, organizations continue to experience significant breaches in endpoint security (Figure 4). More than half of all IT managers surveyed by EMA indicated they had to deal with a malware event (e.g., a virus infection or Trojaned application) in just the last year. Also, 45% reported a device was lost or stolen, which may have placed the company at risk if those devices contained any sensitive data or access to business services. In total, 68% of respondents indicated a security breach occurred in the last year, and these are just the ones they knew about. Far more insidious are security breaches that occur and are not detected by organizations simply because they lack the essential monitoring tools to enable risk management.

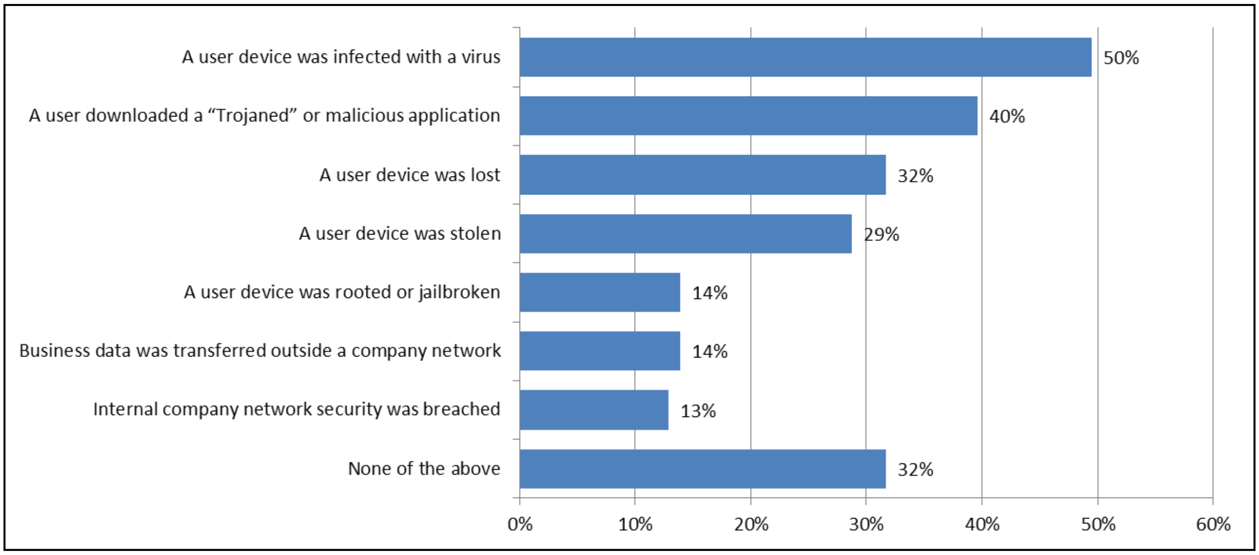


Figure 4: Percent of organizations that had a security breach in the preceding 12 months

At the heart of enterprise security requirements is the protection of business data from inappropriate access; yet 89% of survey respondents reported their users regularly employed unsecure methods for data sharing, such as public email systems (e.g., Gmail, Yahoo Mail, etc.), unsecure public cloud storage, Facebook, and physical media devices (e.g., thumb drives). These data sharing practices take potentially sensitive information beyond the control of the business and can violate regulatory compliance rules or otherwise place the business at risk. Among the most essential practices for data loss prevention is providing users a secure method for data sharing and preventing data from being distributed through alternative avenues. Also, encryption should be applied to data when it is at rest in its hosting environment, in transit to an endpoint, and in use by an application.

Without a doubt, enterprise security is currently the primary focus of enterprise IT management. EMA research has identified it as the practice considered the most important, the most difficult, the most expensive, and the most time-consuming to perform by IT managers. This is no surprise given the frequency of news reports exposing damaging IT breaches in organizations that are expected to maintain high-levels of risk management, such as financial institutions and government agencies. Today’s businesses take the threat of IT breaches very seriously, and their most significant challenge is to prevent risk exposure without reducing application and data availability to authorized users or impacting business performance. While attaining this careful balancing act is not unattainable, it is not achieved without considerable efforts, so ease of use in security management practices is also of paramount importance.

Administration Efforts

There can be no question that IT administrators are excessively busy supporting the constant barrage of end-user requests and business requirements. Among the many management practices, security accounts for the most administration time, with one-third of survey respondents indicating security tasks take a significant amount or the majority of administrator time to complete (Figure 5). This is somewhat counterintuitive considering two-thirds of respondents indicated they employ automated security management solutions. Either these adopted solutions are insufficient to support all endpoint security requirements or they are too complex to operate in a reasonable amount of time. Organizations that spend significant amounts of time meeting security requirements should invest in a more robust monitoring, authentication, and risk mitigation platform to simplify support requirements and improve operational cost-effectiveness. Additionally, real-time response to security threats is essential to reducing or eliminating breach events. The longer it takes to identify potential risks and remediate security threats, the more likely it is that an attack will be successful.

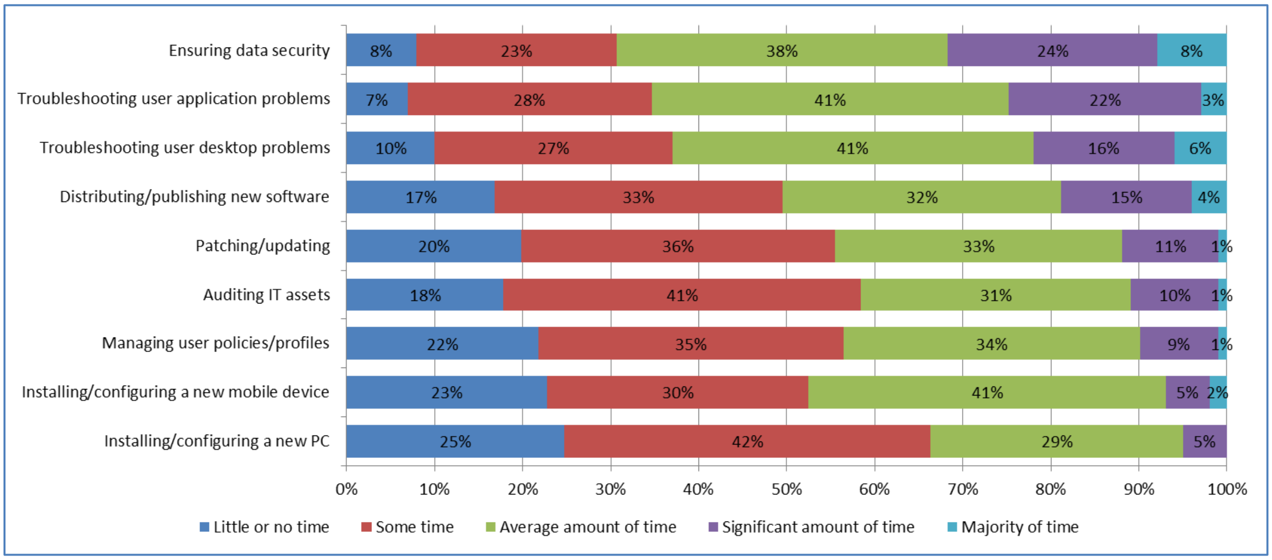


Figure 5: Amount of time administrators spend supporting key management processes

Troubleshooting user application and desktop problems were also noted as being very time-consuming. This is particularly true for organizations that rely on manual process to resolve user challenges. Diagnosing problem on remote devices can be very difficult if administrators are unable to view endpoint configurations and status information. Additionally, administrators trained to support only one particular platform (most frequently Windows) are increasingly challenged to resolve issues on other devices. It simply takes longer to perform unfamiliar tasks than familiar ones, and this difficulty is exasperated if multiple interfaces need to be accessed to diagnose and remediate problems on heterogeneous devices.

Unified Endpoint Management

Overcoming the challenges of enabling security and user productivity in an age of workforce mobility and multi-device support requires a fundamental shift from traditional endpoint management processes. Mobile management platforms were initially developed and introduced independently from well-establish PC management solutions, and in many organizations these solution sets continue to be managed separately. The utilization of multiple consoles to perform related administrative tasks (often called "swivel-chair management") is inherently inefficient and ultimately unsustainable in the face of accelerating requirements for supporting workforce productivity. EMA's research indicates that this is particularly true with the attainment of endpoint security, which was determined to be the most important management service to surveyed respondents and the most challenging to perform.

An ideal user device support approach employs a single console interface and a common asset database and reporting engine to enable unified endpoint management for all devices in the support stack. Principally, this involves providing extensible support for non-Windows architectures, such as Mac, Android, and iOS devices. Additionally, a unified endpoint management approach must include fully integrated support for security assurance. In this way, administrators can employ a common set of processes for recording device information, patching and updating software components, provisioning applications, and ensuring continuous security compliance. Additionally, a single set of user profiles defining access rights, privileges, and default configurations can be maintained for all supported device platforms to ensure consistency and eliminate duplicate management efforts.

EMA Perspective

The key to simplifying the management and security of heterogeneous user devices is the adoption of a unified endpoint management platform. However, selecting a solution should not be a process taken lightly. Organizations should look for platforms that provide fully-integrated support for all endpoint devices in their support stack, rather than a collection of point solutions that are simply accessed from a common console. In particular, it is becoming essential for support to be provided for the growing number of business-employed Apple devices. Functional integrations must include consolidated data collections on endpoint configurations, software, and performance status, which can enable holistic reporting and alarming for prompt identification of issues and root cause analysis. Also, it is critical for that platform to incorporate all automated security management practices to reduce the complexity of risk mitigation. A policy-based approach will ensure a single set of profiles can be maintained for all supported users and devices.

A unified endpoint management solution not only reduces administration efforts; it is also essential to creating consistent user experiences. User productivity is significantly boosted when they can focus on the job tasks they need to perform rather than how to access them. When business application, data, and services are accessible in a predictable way, with the same restrictions and access requirements for all devices, users are liberated to employ any device they find most appropriate to their current location and the tasks they need to perform. In this way, IT services are directly aligned with business requirements to deliver a more efficient and cost-effective approach to client lifecycle management that addresses the demanding service delivery challenges of a mobile workforce.

About Ivanti

Ivanti is IT evolved. By integrating and automating critical IT tasks, Ivanti is modernizing IT and helping IT organizations successfully navigate digital workplace transformation. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.