UBM

7 End-User Computing "Musts" for the Windows 10 Workforce

January 2017

Microsoft's OS offers new opportunities for ensuring productivity anywhere and security everywhere. Here's how to take maximum advantage of those opportunities.

The workplace has changed radically. People now move fluidly among desktops, laptops, tablets, and smartphones — as well as across networks and locations — as they try to keep up with the intensifying demands of work and life. They're also using a larger set of constantly changing digital resources, including both traditional and cloud-based apps. And on top of this, with the advent of agile and continuous delivery, both apps and operating systems require more frequent updating.

Conventional approaches to desktop management and mobile device management (MDM) are no longer adequate for this new digital workplace. Enterprise IT must quickly and dramatically change the way it manages users' access to digital resources to deliver a consistent experience across all devices, even as operating systems and platforms relentlessly evolve.

Failure to adapt to the new rules of digital work with a fully unified approach to endpoint management will result in productivity shortfalls, weaker security, compliance failures, poorer employee engagement, and reduced returns on technology investments.

Fortunately, with the advent of Windows 10, IT now can rethink the way it aligns endpoint management with users' new digital work styles. Specifically, IT can adopt unified endpoint management (UEM) that takes conventional group policy practices to the next level with new "push" capabilities and context awareness that more effectively support the new digital workplace.

With Windows 10, IT can adopt unified endpoint management that more effectively supports the new digital workplace.

7 Musts for the Windows 10 Workforce

Seven "musts" can help IT fully leverage Microsoft's newest operating system to better serve the business.

1. Unify desktop and mobile management silos

Central to the concept of UEM is the elimination of desktop and mobile management silos. Logically and functionally, an endpoint is an endpoint regardless of its form factor or type of network connection. And users need to get the same work done regardless of whether they're in the office or elsewhere. Therefore, it makes sense to take a unified approach to providing them with access to the apps and resources they need across devices.

Several recent developments facilitate this unified approach. One is the introduction of MDM APIs as a new standard for managing the OS. These APIs allow IT to move from traditional Group Policy Object (GPO)-based management that was primarily suitable for devices on domain with fixed network connections to a mobile/cloud model that can be applied more universally across platforms and without network and domain dependencies. Another is the introduction of a unified set of APIs (part of Windows 10 Universal Applications), which lets a single code base run and be easily deployed and managed on any Windows device.

Sponsored by

vmware airwatch

By understanding and taking advantage of these new Windows 10 administrative capabilities, IT can begin a shift to UEM. As organizations move to this new model, for some time at least, IT will also require the ability to complement these modern UEM efficiencies with traditional PC management functions (e.g., support for GPOs, scripting and task sequencing, and Win32 app packaging and deployment) from the cloud as required. That’s a win-win for both the business and the endpoint operations team.

2. Rethink onboarding

Historically, IT has onboarded new devices through a pre-staged imaging process that consumed IT resources and delayed delivery to the end user. But slow onboarding is no longer acceptable. Businesses need new employees to become productive right away. Millennials expect IT to deliver the same ready-out-of-the-box service model for PCs that they have for their smartphones. And IT has lots of other things to do besides load images onto devices.

By providing an OS that can be trusted to connect safely to the network right away — and that then allows devices to fetch appropriate binaries, settings, and permissions over the air — Windows 10 offers an environment that is highly conducive to this kind of streamlined onboarding.

To take advantage of this more efficient onboarding model, IT must redesign its approach by moving from device imaging to workspace provisioning. Typically, this entails creating a set of digital workspace templates that users can retrieve automatically based on their identities, roles, OS platform and version, and various other criteria. An automated workspace retrieval repository also lets IT update new workspace “products” faster, more frequently, and with greater granularity than it has in the past. In this way, it can better keep in step with rapidly changing business and technical requirements.

An automated workspace retrieval repository lets IT update workspace “products” faster, more frequently, and with greater granularity.

3. Intelligently define policies for immediate, automated extension everywhere

Most IT organizations haven’t been able to adopt a full policy-based approach to endpoint management. That’s in part because individual policy attributes have had to be implemented in a highly fragmented manner: permission to access a SharePoint instance here, a geo-fencing restriction there, and so on. Use of policies has been undermined by the fact that it takes so long to roll them out across large numbers of devices both on and off the enterprise network, which must also be restarted before new or modified policies can take effect.

To overcome these obstacles, IT needs to implement true policy-based endpoint management that provides a unified point of control for all policy attributes — via modern MDM, traditional GPOs, or both — everywhere. IT is then able to define complete policies for access, authentication, encryption, whitelisting, context-based session controls, and more across all Windows devices and devices running other OS platforms (e.g., iOS, Android, macOS, and others) within and beyond the enterprise perimeter. And it can do that with confidence that those policy settings will take effect immediately.

4. Enable contextual self-service

With effective policy management in place, IT can more aggressively move to a self-service model that lets users add permitted apps and resources to their digital workspaces. That’s because the policies ensure that users can’t self-authorize any apps or resources they shouldn’t access.

IT must facilitate self-service by making it easier to create application store portals that let users access available, permitted applications — including traditional Win32 and new Windows Store apps, commercial third-party software, internally developed applications, software as a service, and published remote apps — based on their identity, roles and responsibilities, and location, etc. IT can also create policies for these stores that safeguard license compliance while optimizing concurrent use through license recycling and reclamation mechanisms.

The result is a more consumer-like user experience that optimizes employee productivity while reducing IT’s administrative workloads.

5. Maintain OS updates without the stress of Patch Tuesdays

It’s important for security and support purposes to keep endpoint OS versions up-to-date. But the traditional bulk Patch Tuesday model is disruptive and inefficient. It also limits the frequency with which IT performs updates, creating large windows of vulnerability and delaying implementation of new OS features.

As the enterprise migrates to Windows 10, IT can now take control of its update cadences by more flexibly defining policies for update execution. Feature upgrades can either be deployed immediately along with critical security updates (“Current Branch”), with a slight delay to allow for pre-deployment testing (“Current Branch for Business”), or at a time of IT’s choosing (“Long-Term Servicing Branch”) for especially sensitive deployments such as medical and financial systems.

While Windows 10 makes it easier to overcome the bulk patch problem by allowing continuous, over-the-air updates, IT still needs a UEM solution that supports granular updates of the OS on all devices everywhere and on any network, as soon as they become available. This keeps endpoints uniform without disrupting user productivity. It also minimizes security vulnerabilities by eliminating delays for critical fixes.

A UEM solution that supports granular updates of the OS on all devices and networks keeps endpoints uniform without disrupting user productivity.

6. Leverage policy automation and reporting to simplify compliance

Compliance is becoming a bigger burden on IT as the enterprise environment becomes more complex. This burden is compounded by manual processes that are not self-documenting and by endpoint management tools that produce fragmented reporting.

UEM dramatically reduces this burden in several ways. First, it provides a centralized, automated mechanism for defining and enforcing compliance-related policies everywhere. Second, it provides unified visibility into all endpoint devices so that IT can easily discover and automatically remediate compliance-related anomalies in those devices.

Third — and often most important when a compliance audit occurs — UEM lets IT consolidate compliance-related reporting. This unified reporting makes it much easier to quickly provide auditors with the documentation they need to give IT a passing grade. Unified reporting also tends to be much more credible to auditors because it eliminates the multiple data consolidation steps that can introduce errors and inaccuracies into compliance documentation.

7. Establish privacy capabilities that allow mixed business and personal use of devices

Enterprise IT must come to terms with mixed business and personal use of mobile devices. It can do this by adopting a formal bring-your-own-device program, by setting guidelines for personal use of corporate-owned devices, or by some combination of the two. But any approach to mixed use requires secure abstraction of the employee’s digital workspace from the underlying hardware.

Windows 10 facilitates this abstraction by containerizing work-related apps, content, and connectivity. The OS identifies corporate content based on attributes such as source file server, mail server, IP address, and DNS address. That content can then be automatically placed in its own container and encrypted with no disruption to the user experience. This allows policies and administrative actions (such as remote wipes) to be aimed at business containers, without affecting personal content.

These technical capabilities are extremely valuable given how boundaries between work and personal life are becoming more blurred. Privacy safeguards are also increasingly important given how high turnover and the growing use of contractors affect data governance, as well as the likely impact of regulatory mandates such as the European Union’s General Data Protection Regulation on employer-employee obligations. To effectively address these issues, IT must properly define and automate all relevant policy parameters.

The Value of UEM

The investment in UEM and policy automation is well worth it. Work is being radically transformed by digital technology — which is itself being radically transformed by ubiquitous mobility. By embracing the seven practices outlined above, enterprise IT organizations can gain multiple important benefits, including the following:

- **Greatly reduced endpoint administration.** With limited head count and budget, IT won’t be able to afford endpoint ownership costs that keep rising unchecked. UEM with Windows 10 takes time and operating expenses out of the endpoint equation — allowing finite resources to be allocated elsewhere.

- **A better end-user experience.** The more quickly IT can give employees what they want and need, the more productive they can be. And that productivity translates directly into happier customers, increased innovation, and improved business performance.

- **A safer enterprise.** Inadequately governed endpoints are a tremendous threat. Unified, well-automated endpoint controls significantly reduce associated security and compliance risks without impeding productivity.

- **Enhanced business agility.** Businesses can’t move fast if their delivery of digital capabilities to end users is slow. By taking multiple sources of friction out of digital delivery, UEM and Windows 10 enable this essential agility.

Wayne Gretzky famously shared his father’s advice to “skate to where the puck is going, not where it has been.” The same is true for endpoint management. IT must get ahead of endpoint transformation or face consequences that include higher costs, more frequent cybersecurity breaches, and a frustrated millennial workforce. Properly implemented and managed over time, UEM and Windows 10 offer an extremely compelling alternative.

VMware AirWatch: The Leader in Unified Endpoint Management

VMware AirWatch enables true user-centric management for all your endpoints in a single solution. It uniquely allows you to manage the complete device lifecycle from onboarding to retirement across all your desktop and mobile devices, including Windows, macOS, Android, iOS, QNX, Tizen, and Windows CE — as well peripherals and Internet of Things devices such as wearables, printers, and kiosks. No other UEM solution gives you greater control and more effective policy-based automation over everything from application permissions to encryption policies.

Try VMware AirWatch free for 30 days. Click here for details.