WHITE PAPER–SEPTEMBER 2020

Modernizing EUC Management: From Device Provisioning to Enrollment

Foundational digital workspace journey milestones

vmware®

Table of Contents

Executive Summary

The workplace is radically changing: more applications are in the cloud or offered as services, more employees are working remotely, and more workers want flexibility in device choice. In light of today's workplace applications, devices and work styles, device and image-focused management is too time consuming, resource intensive and limiting. To simplify overhead and expand device and work options, organizations are reevaluating their established tools and processes for provisioning, managing and securing endpoint devices. By shifting to a lighter management model for end-user computing (EUC), organizations can keep pace with the faster evolution of workspaces and enable employees and IT to be more agile.

Implementing a lightweight management approach is more than just changing tools. It also requires modernizing processes, acquiring new skillsets, and revising roles. These changes affect everything from application deployment and testing cycles, engagement with business units, and how information is communicated to IT and respective business units. This modernization will primarily impact desktops and laptops running Microsoft Windows, which are a majority of the computers in use and account for a significant share of IT operational overhead. By reducing device-level operational overhead, employees take a more active role in managing their workspaces, and some IT professionals alter their job functions, which typically requires a carefully managed transition.

Many organizations are hesitant to modify well-established processes in fear of the disruption that this might cause. However, these older processes have several limitations that over time will constitute a barrier to effectively manage the modern workspace. Mainstream device operating systems, like Windows, are evolving rapidly with shortened periods between releases. And employees are demanding more device and platform choices. As the traditional processes make it more challenging and costly to adapt, the issue is not whether to move to a lightweight management model but when and how.

It is time to seize the opportunity to achieve the gains from modernizing EUC management. This paper describes some steps and considerations that your organization can take to augment or replace your existing processes with dynamic ones and minimize disruption.

Recommendations

To reduce management overhead and keep pace with the changing workspace:

- Shift the focus of workspace management from devices and system images to users and entitlements.
- Adopt unified endpoint management (UEM) tools to support the constant change that occurs at the device, user and policy levels.
- Transform the provisioning, configuration, application management, patching and security of your digital workspaces by adopting user-centric, dynamic processes.
- Align key stakeholders on a unified approach to workspace management and security. Establish new levels of collaboration with the security and application teams.
- Help EUC engineering, IT operations and support team members understand the organizational and professional benefits of enabling a dynamic workspace evolution. Provide access to the tools and the knowledge needed for this transformation.
- Encourage a more proactive role for employees in the onboarding and management of their workspaces. Plan to communicate and educate employees accordingly.

Managing a Modern Workspace with Old Processes Does Not Work

Since the mid-1990s, organizations have managed and secured PCs by tightly controlling their configurations. PC lifecycle management (PCLM) tools, introduced to manage OS and application deployments and updates at scale, require that every configuration be "known" so that management processes can be applied predictably. As this approach became best practice, the goal of many IT departments was image standardization, which impacts how devices are procured, managed and secured.

As application complexity and the variety of devices grew, operational costs rapidly increased. In best-practice organizations today, PC operational costs are usually at least four times more than capital costs, and the user-to-IT staff ratio is typically 250:1. This overhead motivates organizations to restrict the number of configurations, which in turn creates a barrier to change.

This rigid model for managing PCs also does not support employees' demand for more device and platform choices nor can it keep up with the more frequent updates of modern operating systems. To support a greater diversity of work styles, applications and device types, unified endpoint management (UEM) has become a popular approach to lightweight management that is not bound to a particular type of device. UEM enables IT to manage, secure and deploy resources and applications on any device from a single console. Instead of provisioning PCs by building images, establishing staging servers, relying on complex and heavy PCLM infrastructures, and being limited to preconfigured standards, organizations can use UEM tools to securely enroll any device—such as a Windows 10, macOS or Chrome laptop, including those that are part of a bring-your-own (BYO) program—and reliably deliver applications, data and personalized settings to it.

The advantage of a lightweight management approach is its simplicity when supporting fast-evolving environments. For instance, when managing mobile devices with UEM, one IT staff person can typically support 2,000–5,000 users, despite fast refresh cycles of 18–24 months for mobile devices and platforms. By applying a lightweight approach to PC management, similar benefits can be obtained.

Because traditional PC management processes are highly entrenched in EUC teams and the skillsets of IT practitioners, many organizations are reluctant to face the possible disruption caused by modernization. But over time, these older processes will become a barrier in effectively managing the modern workspace.

Managing a Modern Workspace with UEM

Traditional processes hinder device and platform diversity, do not fully support a distributed workforce, and expand the cost of managing OS and application updates and adoption. In contrast, when using UEM for device deployment and management, you can fulfill employee requirements more granularly. Instead of a "take it or leave it" approach, which is common in many organizations that use imaged PCs, provisioning can be based on a user's specific needs and requirements. An individual's profile rather than a device's profile determines which applications and services are delivered. As a result, organizations can fit technology to user workflows and requirements in a more dynamic, responsive, and agile way.

UEM overcomes the rigidity of traditional PCLM tools and processes in several ways.

Device and platform choice – Employees want a greater choice in how they work, and PCLM tools, coupled with traditional processes, present a roadblock in enabling employees to use personal devices for work. Managing PCs through standard system images and hardware is an obstacle to adopting a greater diversity of device types, form factors and platforms because each system introduced substantially increases the work required to manage the PC environment.

Unified endpoint management works across multiple platforms, enabling you to configure, control and monitor a wide range of devices from a single management console. Because configuration processes can be predicated on user-based policies rather than on the underlying hardware configuration, organizations can enable different device ownership models, ensuring that policies follow users on any device.

Distributed workforce – With today's mix of working remotely, from home, and on premises, OS updates, application delivery and device security need to be provided in ways that are independent of location and network. Traditional PC management processes, especially those related to patching and application management, are increasingly out of sync with evolving employee work styles because they are designed to manage devices on the corporate domain and network and are tied to traditional network architectures.

A modern management framework based on UEM overcomes these limitations by keeping all endpoints, whether in the office, remote or in the field, up to date and compliant with corporate policies. New processes can be established to onboard, distribute applications, give secure access to corporate resources, and monitor and support a remote workforce.

OS and application management – Modern operating systems evolve through smaller and more frequent updates that target security fixes and feature enhancements. Old PC management processes were designed for platforms that evolved through major releases that occurred every 3 to 5 years. According to industry experts, the work required to absorb frequent OS updates using traditional PC management processes and to test and pilot applications against new releases increases management costs.

Under a modern management model, not only is the cost of absorbing OS updates lower, but support, administration and deployment also present less overhead.

TCO Savings with Modern Management

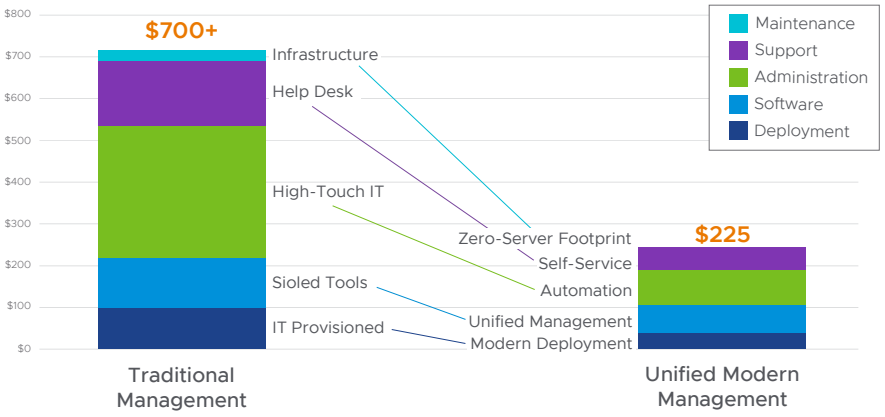

Figure 1: Traditional and Modern PC Management Cost Comparison

Indirect costs, or the lost productivity due to downtime and the time spent by users trying to resolve their own issues, are also reduced because devices running dynamic operating systems and their associated applications are generally more reliable than those with static configurations. PCs can increasingly be considered as appliances, and users can quickly swap devices, so the downtime and lost productivity due to an inoperable device are minimized.

How Management Processes Change

Implementing modern management means augmenting existing processes or replacing them with dynamic ones. These changes affect everything from application deployment and testing cycles, engagement with business units, and how information is communicated to IT and respective business units.

	Traditional PC Management	Modern PC Management
Deployment	High-touch imaging	Faster onboarding options, including self-service enrollment.
Configuration	On-network GPOs	Configuration based on profiles and cloud policies defined in conjunctiuon with security team and business managers.
Patching	Monthly patch roundup	EUC establishes how and when updates are applied and determines distribution rings. Greater reliance on users testing.
App Management	Resource intensive packaging	EUC to build and maintain a comprehensive self-service applications catalog, based on users' entitlements defined by the business.
Security	Reactive	Proactive. Requires greater understanding of users work styles, applications and data requirments.

Figure 2: How Traditional Processes Change with Modern Management

Dynamic processes reduce overhead, improve agility and introduce security benefits, but transitioning to the new processes also requires reorganizing the EUC team and rebalancing skillsets. IT skills in new tools and approaches need to be expanded while those based on PCLM processes will be in less demand.

Deployment – The labor-intensive and costly processes of PC imaging and domain joining are replaced by an enrollment process that can be applied over any network and across corporate and personal PCs. As a result, new onboarding options become feasible. For instance, employees can receive a ready-to-work PC directly from the manufacturer. Or they can take advantage of self-service enrollment by using their work credentials to join devices to a cloud domain and then pull down their profile, settings and applications. These processes reduce IT involvement in provisioning while delivering a more effective and automated onboarding experience to employees. These options are especially important for organizations with a distributed workforce.

This shift means selecting the onboarding workflow that best suits the organization and its use cases, introducing new tools to replace or work alongside PCLM tools and redesigning enrollment processes accordingly. Some onboarding options could be implemented by the employee, requiring new levels of training, communication and guidance.

Configurations – Under modern management, profiles provide the primary mechanism for managing devices. A profile consists of settings, configurations and restrictions. When combined with compliance policies, the profile enforces corporate rules and procedures. The EUC team can deploy policies via the cloud to remote workers.

Migrating Group Object Policies (GPOs) to a modern management framework can be complex because, in many cases, GPOs contain remnants of older OS versions, applications that have been decommissioned, and other past IT projects. To address the complexity, the EUC team needs to identify the policies that are still relevant and decide on the best approach to configure them under modern management. Creating and managing user profiles and policies requires close collaboration between the EUC team, security and access team, and line-of-business managers to establish and manage user entitlements.

Patching – Patching changes significantly with modern management. The EUC team leverages Windows as a service framework and chooses when and how updates are applied to devices over the air. Updates can be scheduled, forced, or allow the end user to choose when within a period of time set by IT.

For the EUC team, these changes reduce effort because of a greater reliance on the OS vendor and more employee involvement. The EUC team determines the amount of time required to test and deploy updates. With a faster update cadence, application performance needs to be tested more regularly, so investments in automated testing and DevOps are likely needed to reduce the burden on IT. The EUC team creates and updates distribution rings for Windows patches and defines which updates can be automatically approved by the administrator. The move to cloud-based patch management requires greater agility from EUC teams and active engagement with business units in managing and signing off user acceptance testing for new versions of business applications.

Application distribution and management – The shift to modern management is an opportunity to modernize and automate the mechanisms for delivering and managing applications. The self-service application model fits well in an environment that evolves quickly and where applications are ideally independent from the OS. Application stores supplied by the OS vendors partially fulfill this role, however a consolidated catalog that delivers applications of different kinds, including software-as-a service, desktop and mobile applications, offers the best user experience and encourages employees to explore new tools for their productivity needs.

Moving to self-service applications means that EUC staff can move their focus toward creating and managing more comprehensive enterprise catalogs that include all application types. In this scenario, business unit managers assume responsibility for defining and managing employee entitlements to applications and access to corporate resources, so they will need training accordingly. Informing and training employees around the new ways for searching and accessing applications will also be required.

Security – Perhaps the most significant area that benefits from adopting UEM is workspace security. PCLM approaches to security rely on reactive tools, such as malware detection and virus scanning, because the primary security goal is enforcement. Security administrators typically use tools like VPN, encryption and group policies as additional layers of protection for users and devices. These approaches are designed for detection after the fact and are, like PCLM techniques, often based on static device configurations and slow to change.

UEM, coupled with modern endpoint security tools, shifts the security posture toward prevention. The concept of zero trust is rapidly emerging as a more effective method for managing access to corporate applications and data, particularly for new and evolving work styles. Zero trust is not a single technology or product but an approach that considers every user and every device to be untrusted until a number of factors have been verified. Only after verification has been completed is access to corporate applications and data granted. Moreover, the requirement of verification is ongoing rather than occurring once.

Access and availability are governed by user permissions, profiles and entitlements, not device type or ownership. Administrators will need to spend more time understanding and addressing user application and data needs. They must also understand the context of where and when applications are accessed or prohibited to ensure that they correctly enable conditional access based on device type, network, location, time of day, and so on. Collaboration with security teams is a must because the creation, management and enforcement of rule-based policies becomes a joint responsibility, especially when embracing identity management. Security is extended to every aspect of the user and device lifecycles, such as onboarding, entitlement, change management, audits, reporting and retirement.

Going Modern

The shift to modern management reduces overhead and enhances agility—for IT, employees, and the organization. To navigate this shift successfully, many processes and best practices need to be reinvented. Using UEM tools to manage all devices, including PCs, does necessitate reorganizing the EUC team and rebalancing skillsets. IT skills in new tools and approaches need to be expanded while those based on PCLM processes will be in less demand. Organizational structures that separate mobile and desktop management functions need to be rethought as the benefits of a single, combined team tasked with supporting all users and devices become more apparent.

Modernization requires careful planning, effective communication and some organizational change. But these changes also provide a foundation for other key steps in the digital workspace journey, such as moving to new application delivery models, modern onboarding, and unified management for all endpoint devices. The benefits will extend beyond the EUC IT team, enabling critically important changes to be made to security, support, and lines of business.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Copyright © 2020 VMware, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: FY21-6019-VMW-MODERNIZING-EUC-MGMT-WP-USLET-WEB-20200908 9/20