IDC ANALYZE THE FUTURE

IDC TECHNOLOGY SPOTLIGHT

Sponsored by: Citrix Systems

Unified workspace management can help accelerate digital transformation in the enterprise by providing end users with secure, on-demand access to the apps and data they need.

The Need for Unified Workspace Management

Written by:

Phil Hochmuth,
Program Director

Shannon Kalvar,
Research Manager

Introduction

Digital technologies and the new business models that they fuel have significantly impacted most enterprises. Executives are called upon to leverage digital transformation (DX) to transform and disrupt their business, customers, partners, markets, and competitors. The subsequent rise of disruptive trends such as the consumerization of IT, bring your own device (BYOD), choose your own device (CYOD), and the Internet of Things (IoT) is driving increasingly heterogeneous and hybrid client device environments.

And as mobile devices, laptops, desktops, and even wearables become more diverse from a hardware and form factor standpoint – and the software and apps running on these devices become more powerful, dynamic, and immersive – enterprises are rethinking the traditional models of IT device management and end-user enablement.

AT A GLANCE

KEY STATS

24.7% of enterprises are using or piloting unified endpoint management (UEM)

41% say they plan to adopt the technology in the next 6–18 months

53% would increase spending on UEM over the next 12 months

KEY TAKEAWAY

More than half of enterprises will need to look at how UEM will affect separate IT deployment, support, and security functions across mobile and PC devices.

Indeed, physical endpoint devices themselves are becoming less critical from a management and policy enforcement standpoint, while data and applications are emerging as more essential IT assets against which access controls, monitoring, provisioning, and other security/management functions are being applied. As devices commoditize, and device ownership blurs between BYOD and corporate liable, identity-based control over apps and data becomes paramount.

Enter the concept of the workspace, the unification of a collection of managed end-user computing environments (i.e., operating systems, applications, data, and data access functions that are centrally provisioned, managed, and controlled with common access control and security policies). By using a digital workspace to mitigate the performance and support dependencies between operating systems, applications, and device types, IT can provide end users with a unified and consistent user experience across legacy on-premises, SaaS, and native mobile applications as well as access to files and collaboration tools seamlessly, often with

April 2018

single sign-on. Furthermore, these digital workspaces can be accessed across mobile or fixed devices, from smartphones and tablets to mobile PCs, fixed workstations as well as within virtualized client computing environments.

Businesses have known for over a decade that "workspaces" are not just places but also collections of apps and services that must be accessible on more than one device type. Today's business users want to create and view information on multiple devices in real time, regardless of location; enterprises want to empower users to accelerate innovation and DX opportunities for business growth. Still, many organizations only deploy one or two parts of end-user workspace technology. And those that have multiple pieces in production rarely have a unified management view of the environment.

Unified workspace management (UWM) is a critical end-user computing management platform that centralizes control over workers' computing environments across multiple device types — mobile, PC, and virtual — and applies common configurations, rules, and policies to apps, data, and systems access across these disparate environments. Such platforms can help accelerate DX in the enterprise by providing end users with secure, on-demand access to the apps and data they need to work efficiently from anywhere, at any time.

IDC believes that IT organizations should be thinking about integrating multiple types of management platforms for disparate end-user computing technologies — from endpoint devices and applications (both mobile and PC) to virtualized desktop and apps as well as overall end-user computing work environments. To that end, enterprises should adopt a UWM approach to overall end-user computing environments, encompassing physical and virtual endpoints, applications and data access policies, and software distribution and version control.

Definitions

Future of work: Existing shifts in demographics, economics, and technology will drive fundamental changes to the nature of work. The key word in this change is emergent – emergent value, emergent processes/products, emergent networks of action (ecosystems). That changing nature of work will be constrained at first by technology but those limits will fade and leave behind limits in design skill and imagination which will persist over time.

Virtual client computing (VCC): IDC defines the VCC functional market as a client computing model that leverages a range of brokering software and display protocols to enable server-based client computing and improve upon the limitations associated with the traditional distributed desktop environment. The VCC market includes products that enable the configuration and management of centralized virtual desktops, virtual user sessions, and other forms of client virtualization to include type 2 hypervisor, containerized, and cloud-based solutions for delivering virtualized desktops and applications. Management software specifically targeted at the configuration, control, and operations of VCC solutions is included in this market.

Full VCC life-cycle management: There are four phases (procure, provision, operate, retire) in the VCC life cycle. Procurement of both physical and virtual resources for client computing must increase in speed and simplicity to both decrease time to the next step (provision) and reduce the time/money cost of transitioning from one device/operating system to another. Provision is one of the largest efforts in the endpoint/client computing operations life cycle, and it allows IT staff to ensure proper hardware configurations and software currency/licensing, manage user access, and demonstrate compliance. Operation of hybrid (physical/virtual) clients includes the integration of applications, compute, data, workflows, and other resources first within and then across enterprise boundaries in a fashion sustainable across the lifespan of the requirement. Retire has traditionally been a weakness of virtual client computing software. Virtual clients might linger on long past their actual use; physical devices can continue in use long past the theoretical lifespan. Access is challenging to control and as the underlying assets providing compute have moved from datacenters to hybrid clouds exactly matching compute expense to usage has become a concern.

Unified endpoint management (UEM): UEM represents a holistic approach to managing physical desktops and laptops, mobile devices (smartphones and tablets), virtual client computing environments, and emerging IoT endpoints, such as wearables and smart connected devices. UEM allows the consolidation of two separate previous device management platforms — PC life-cycle management (PCLM) and enterprise mobility management (EMM). This consolidation to UEM sets the stage from an endpoint control perspective for modern workspace management. Having all endpoints managed on a single platform — the proverbial "single pane of glass," finally realized — can consolidate the metrics for assessing how client devices deliver hardware and software discovery, control, configuration, and monitoring capabilities. Unique KPIs for UEM enable a business approach in determining the DX value of physical desktops, virtual desktops, tablets, smartphones, and the increasing presence of IoT devices. The consolidation to UEM also provides advantages from a security and visibility perspective, allowing for common, consistent polices to be deployed across any endpoint form factors. According to IDC research, more than two-thirds of enterprises plan to move to a UEM model over the next two years.

Unified/virtualized application and data delivery: The utilization of VCC software to support application and data delivery to mobile workforce environments continues to be a market growth driver. Enterprises continue to seek solutions that allow for the efficient and secure delivery of corporate information across varying device types.

What Is Unified Workspace Management?

The workspace is a loosely defined industry term implying a unified end-user experience and management platform for desktop, mobile, enterprise applications, and data/content access tied to end-user identity and role. In essence, the workspace serves as an abstraction layer between devices, active directory, and user policies, allowing access policy management to be centralized for all applications across multiple clouds and on-premises architectures. Likewise, as workspace offerings mature, it is expected that they will become increasingly integrated with adjacent technologies to tailor the workspace for specific use cases and/or industry verticals.

The workspace concept will likely drive continued adoption of EMM and VCC in the near term, as businesses discover ways to integrate and unify mobile and traditional endpoint computing experiences and tie solutions to application access management technologies via identity platforms. Cloud will be an important component of this, as workspaces access will be required from any device or location. Vendors with the complete workspace stack have PCLM, application distribution, VCC deployment and management, EMM, and identity and access management platforms.

Workspace Management Includes UEM and Other Functions

UEM is the convergence of traditional PC management platforms with centric management technologies such as mobile device management (MDM) and EMM. In addition to converging the types of devices managed, UEM also shifts enterprise end-user computing to more open, cloud-based frameworks. IDC sees 2018 as a pivotal year for UEM technology development and enterprise adoption.

Indeed, the coming year will represent a “bridge” for most enterprises regarding UEM deployments. Over the next 12 months, businesses will use both existing mobility and traditional PC management platforms, tying these together in smaller pilots of unified management, focused particularly around Windows 10 deployments.

Modern PC management is mostly associated with Windows 10 and the use of the operating system’s (OS) underlying management APIs and framework for endpoint device configuration, policy enforcement, and security and compliance checks. Modern management uses hooks in the OS itself, instead of PC-based agent or client software, to manage devices, which can be done over the air and via the cloud, as opposed to requiring devices to connect to private networks for management and configuration. PCLM technologies, a traditional enterprise endpoint technology, use a server/agent-based model to push policies (i.e., Windows Group Policy Objects) to endpoints. Windows modern management, sometimes referred to as "Windows MDM," can be controlled via multiple vendors' EMM platforms, which leads to the concept of UEM, or the control of both PC and mobile devices via a single system.

The organizational change UEM forces will look familiar to any veteran CIO or IT professional who lived through similar convergence trends such as IP telephony (forcing LAN and PBX teams to mix) or datacenter hyperconvergence (the collapsing of storage/compute/network). Such developments have always forced disparate IT groups together. As part of the IDC MarketScape: Worldwide Enterprise Mobility Management Software 2017 Vendor Assessment, more than half of the 20 IT organizations IDC spoke with in the study said their EMM deployments were managed and deployed out of their desktop management or end-user computing IT teams, as opposed to a mobile-specific or telecom-focused IT resource group. This means more of a change in tools, as opposed to teams, will occur in many organizations as enterprises move to modern management of all endpoints. According to IDC's 2017 Enterprise Mobility Survey, nearly a quarter (24.7%) of enterprises are using or piloting UEM, with another 41% of businesses saying they plan to adopt the technology in the next 6–18 months. (More near term, 53% of enterprises said they would increase spending on UEM over the next 12 months.) This means that more than half of enterprises will need to look at how UEM will affect separate IT deployment, support, and security functions across mobile and PC devices. Convergence of tools usually implies a convergence of roles or, at least, the integration of one group into another and the sharing of a single platform among the converged team.

As endpoint management consolidates, management of the security tools touching these endpoints will also come together. Endpoint security has always been tied closely to endpoint management as OS patching, software upgrades, and endpoint maintenance are critical to good enterprise security hygiene and are often managed by security and vulnerability management platforms that integrate with PCLM tools. Teams responsible for endpoint security software and management often overlap and use cross-functional tools. We see this emerging on two fronts in the endpoint management market: businesses are increasingly deploying both EMM and mobile threat management (MTM) together.

However, as mobile security software deployments become more prevalent, businesses will need tighter coordination and management of settings and polices across both mobile and traditional endpoints. More importantly, the ability to correlate threats across these platforms will be even more critical, especially as the lines blur between traditional and mobile endpoint computing devices.

Finally, as automation, artificial intelligence (AI), and interconnected data sources become more critical parts of IT operations, UEM platforms must evolve with these types of analytics and data-driven features to keep pace. The use case for intelligence in security monitoring and management scenarios is also compelling, as security, end-user computing management, and compliance continue to converge in terms of responsibilities, toolsets, and teams.

Forward-looking enterprises will want to consider solutions that will also address advanced cloud computing, cybersecurity, and machine learning as part of an intelligent security framework geared toward allowing IT organizations to secure and simplify access and control of the applications and data.

The Road to a Unified Workspace Depends on the Starting Point

The lofty vision of a unified workspace, adaptive to context and seamlessly integrating digital with physical assets across enterprise boundaries, is both technically daunting and practically challenging. The first steps on the journey are based on which challenge the enterprise needs to address first, then next, with each pool of work bringing discrete value. These challenges are generally grouped as shown in Table 1.

TABLE 1: *Unified Workspace Challenges*

Requirement	Challenge	Program Tranche
Agility	Reduce the cost of operating environment introduction/transition	Unify management and tools
Security	Dynamically manage endpoint risk	Enable security
Utility	Ensure that workspace use-cases adapt to enterprise context	Create hybrid workspace

Source: IDC

Although the work of each pool can be done piecemeal, all three are enhanced if the organization has already adopted hybrid cloud management practices. These practices allow the enterprise to abstract away from specific hardware stacks, focusing attention on the work of the tranche. The tranches are discussed below.

Create Hybrid Workspaces (Addresses Utility)

A hybrid workspace is one in which an array of configurable, context-aware physical and virtual resources can be quickly marshalled to enable a productive user journey. Although it is tempting to think of this in terms of augmented reality and mobile computing, it can be achieved practically through any combination of methods that improve user access to the correct information, in a presentation the associate can consume to make decisions that drive business outcomes. The work here includes but is not limited to:

» Identifying user journeys not being met in current enterprise, partnerships, and supply-chain relationships

» Developing and maintaining both a physical and a virtual client compute approach while provisioning primarily in the virtual world

- Streamlining application sets to enable user journeys, reducing the need for general function virtual desktops
- Developing and maintaining multiple access methods for critical enterprise functions
- Integrating the retirement/shutdown of virtual assets into the productive user journey rather than making it a separate function

Enable Security (Addresses Security)

Enterprise security is growing increasingly complex, both in terms of its requirements and the tactical/technical details of its execution. This complexity, unfortunately, increases the risk the enterprise faces, creating a seemingly never-ending loop of challenges. IDC research indicates that organizations which address these challenges by simplifying their policy, access management, and security integration can thrive in the emerging digital landscape. This work includes but is not limited to:

- Possessing a common policy framework that allows creation and management of common policies regardless of device type, platform, or application
- Creating common identity-driven access management policies across mobile, virtual, and traditional endpoint computing (separate devices from apps + data)
- Deploying services and apps (file sharing, collaboration) to any user on any device type with inherent, seamless security
- Gathering and aggregating data from across the system to identify, pattern, and detect deviations in system or user behavior

Unify Management and Tools (Addresses Agility)

Currently, organizations struggle with multiple device form factors and compute delivery methods because they have separate policies, procedures, and toolsets for each specific case. This creates a highly fractured and complex response, greatly increasing the cost of operating the organization's endpoints and the time required to integrate new devices/platforms/operating systems. IDC research indicates that organizations can simplify this by:

- Combining and managing all endpoints through a single policy and procedure throughout the procure, provision, operate, and retire life cycle
- Combining device management and provisioning of smartphones, tablets (both corporate liable and BYOD) with corporate PCs (and BYOPC) with UEM
- Unifying virtual app/desktop management with mobility and endpoint device management and mobile application provisioning and control thus creating a single console for life-cycle management

Considering Citrix Workspace Solutions

Citrix integrated workspace solutions include Windows app and desktop delivery from XenApp and XenDesktop, device security from XenMobile, secure file sync and sharing with ShareFile, and network security with NetScaler. These traditional products are augmented through the Citrix Analytics and Citrix Cloud offering to create a modern, manageable workspace solution.

Citrix solutions are in use by more than 400,000 organizations including 99 percent of the Fortune 100 and 98 percent of the Fortune 500. This extensive installation base allows Citrix to serve roughly 100 million users through its XenApp and XenDesktop products. It also enables a broad, rich talent pool both for enterprises looking to hire resources to support installations and partners looking to integrate the Citrix platform into hybrid digital/physical workspace solutions.

Challenges

For Citrix, the greatest challenge in UWM will be providing customers with a consistently themed, well-integrated package of workspace products that span its wide range of offerings and technology categories. Citrix has spent more than a decade developing, acquiring, and integrating all the components of UWM. Citrix customers can't be left to piece together the puzzle themselves, especially as they undergo UWM-related organizational and support challenges themselves. Creating a true UWM offering will involve precise coordination among Citrix product/engineering, sales, and the channel. Lastly, in its execution of UWM efforts, Citrix must view UWM as not just an opportunity to cross-sell/upsell to existing customers but as a methodology to help them digitally transform end-user computing deployments in a meaningful way.

From the customer perspective, the move to digital workspaces and UWM will include multiple technology deployment and integration challenges. What may get overlooked is the challenge that UWM will present to IT and business operations and strategy.

From an end-user perspective, not all employees will be prepared for DX and disruption. Many workers have adapted to be productive and comfortable in disjointed and siloed end-user computing environments, which have existed in IT for years. Quick imposition of a unified workspace could be akin to giving a learner's permit holder the keys to a sportscar. Organizations can get ahead of the perceived workspace learning curve by anticipating how employees use technology today and emphasizing the advantages a unified environment will have on day-to-day tasks (i.e., shorter log-on times, seamless mobile/desktop app experiences, quicker IT problem resolutions, and more).

Challenges will also exist on the IT organizational side. CIOs and other IT leaders will have to deal with these changes, just as they have done in the past.

As mentioned, businesses should anticipate churn and disruption in terms of IT domain cross-over, as separate PC and mobile device teams integrate, if they haven't already. Businesses must also consider what pull-through effect this convergence of functions might have on adjacent services or operational responsibilities. For example, if mobile management teams are merged with PC teams, other mobile-related functions could also fall into a newly converged UEM group such as telecom expense management, mobile voice/data plan management, and other activities generally handled by mobility- or telecom-focused teams. Making these internal IT staffing and organizations adjustments before wider-scale UEM deployment and adoption will help businesses get ahead of disruptive departmental turf battles as well as avoid confusion over system ownership and responsibilities, which could disrupt deployment or support capabilities and hurt end-user productivity.

Conclusion

Enterprises deploying or considering this converged UWM approach must think about how the convergence of PC and mobile device management will affect all aspects of enterprise IT support, management, security, and policy enforcement. Beyond technical considerations, businesses should anticipate how existing organizational structures and centers of ownership will evolve as UWM becomes more prevalent.

Once an organization achieves a level of internal control, it should begin to look closely at existing partnership arrangements to identify areas where it can achieve additional value and reduce risk.

The lofty vision of a unified workspace … is both technically daunting and practically challenging.

Message from the sponsor

For more information, visit https://www.citrix.com/products/citrix-workspace/

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA
01701, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.