Embracing the Digital Workplace with Unified Endpoint Management (UEM)

Table of Contents
Embracing the Digital Workplace with Unified Endpoint Management (UEM) ................................................................. 2
Meet Today's Elevated Self-Service Expectations .................. 3
Automate Every Part of Your Workspace Environment ............... 4
Experience the Advantages of “Single Pane of Glass” Workspace Management ................................................................. 4
More Freedom through Better Security ........................................ 4
Stay Compliant in Any Workspace .............................................. 5
Start Enabling Your Secure, Compliant, and User-Centric Workspaces Today ................................................................. 5
Embracing the Digital Workplace with Unified Endpoint Management (UEM)

As a new generation of workers enters the job market, they are bringing a very different set of habits and attitudes with them—including non-negotiable expectations that they can get their work done any time; from any location; using whatever device, connection, and collection of apps happens to be most convenient.

This mindset has created a major shift in how businesses define the concept of a “digital workspace”—and compelled IT organizations to develop a new approach for delivering resources and information to their users. In the past, a typical workspace was a defined area in an office building where people performed most of their work on a managed, company-owned PC and accessed all of their IT resources and applications over a carefully secured and maintained corporate network. In this type of environment, it was relatively easy to make and enforce rules and strictly control access and compliance. And even when users worked remotely, IT could still call the shots on how users connected to the network and what they were allowed to access.

Like it or not, this kind of orderly, clearly defined workspace—and the “command and control” approach to IT that was typically used to manage it—already seem like quaint relics from the past. Today, at least in the eyes of users, a workspace is virtually anyplace they have access to a wired or wireless Internet connection and a corporate-owned or personal desktop, laptop, smartphone, or tablet. To make matters even more complicated, these users expect a responsive, flexible experience every time they interact with technology. They’re used to finding their own technology solutions, whether it’s downloading an app from a consumer app store, finding and using a cloud-based service, jumping on the nearest public Wi-Fi network to stay connected, or Googling answers to their computer issues.

And if IT can’t deliver the types of flexible, functional experiences they expect, users will simply take matters into their own hands, which creates obvious and unacceptable risks.

So the central question is this: How can your organization provide the kind of “any location, any device, any service, any connection” workspaces your users want—without compromising your ability to keep your organization secure and compliant? The answer requires a fundamental shift in the relationship between IT organizations and the workers they support—from a rigid, “command and control,” device-centric management mindset to a user-centric approach that works to provide safe, appropriate access to any workspace on any device in any location.

The right UEM solution should embrace and enable this kind of user-centric, digital workspace experience by extending several key capabilities to any user, device, and wired or wireless connection:

- **User Self Services** that allow users to get the apps, resources, information, and support they need quickly and easily—so they’re never tempted to take matters into their own hands and work around IT.
- **Automation** capabilities that enable you to manage the increasingly complex mix of users, devices, applications, and information in your organization in less time and with less effort.
- **Single-pane-of-glass** management that consolidates all UEM capabilities and management functions into a single management console. This will give you a complete, integrated, and uniquely user-centric view of your diverse corporate workspaces—and makes it easy to deliver IT services and resources quickly and efficiently.
- **Security** that extends far beyond the boundaries of your corporate environment to give your users appropriate, location-aware access to apps and information from any device over any connection.
- **Compliance** solutions for traditional desktops and laptops, mobile devices, and
applications that never force you to choose between flexible remote access and the compliance requirements of your organization.

The following is a more detailed guide for what to look for in a UEM solution:

The Anatomy of Today's Modern, User-Centric Workspace

USER WORKSPACE

USER SELF-SERVICES
Request, track, activate, print, file share and many more from the workspace.

COMPLIANCE
Assure workspace compliance for your assets, licenses, apps, devices, contracts, etc.

BYOD

AUTOMATION
Workspace automation process for all devices & self-services by selecting any services from any device.

SINGLE PANES OF GLASS
Seamless integration of all IT systems by providing a complete view of the workspace.

SECURITY
Secure the workspace through endpoint security, encryption, location-awareness, wireless security, containerization and many more.

Meet Today's Elevated Self-Service Expectations

Today, self-service is about much more than allowing your users to reset their own passwords. It's about giving them a complete set of tools to solve problems and gain access to new apps and information quickly—from any device or location. Empowering users with a complete collection of self-service tools obviously reduces the burden on your IT department. But it also removes the motivation for users to look for answers and resources from outside, unsecured, and non-compliant sources.

Fast, Automated Helpdesk Support from Any Device with IT Service Management (ITSM)
ITSM should give your users direct, convenient access to a complete catalog of service options from any device. Offer your users a convenient app to create their own service ticket, track the progress of the incident, and interact with the helpdesk team—all without ever having to place a call.

A service catalog also allows you to create a convenient, familiar online store experience where your users can request new IT resources—including hardware, software, and any other assets you make available in the catalog. This makes every interaction with your IT organization as easy as purchasing a movie on Amazon.com. And it makes every part of your helpdesk operation more efficient and effective.

BYOD Made Easy with Mobile Management
How many people in your organization already rely on their smartphones as much or more than their office PCs? We recognize and embrace
this mobile reality, and mobile management makes it possible to turn any mobile device into a secure, managed, and effective business tool—no matter who owns it.

First, effective mobile management should provide your users with the capabilities they need to keep their mobile devices—and the corporate information on them—safe and protected. This starts with the ability to track, lock down, or wipe their mobile device if it gets lost or stolen.

Mobile management should also allow you to create a separate secure and managed container for business apps and information on personal devices. This capability gives users an easy, convenient way to access and use corporate apps and information on their own smartphones or tablets. But it also keeps business and personal apps and information separate, and it wraps a crucial extra layer of management and security around the corporate resources and information you need to protect.

**Access Containerized Apps Quickly and Easily**

Finally, creating desktop containers makes it easy for users to select and automatically launch a variety of services from any device they happen to be using—without any direct involvement from IT.

Together, these capabilities allow you to give your users the kind of easy, convenient, and complete self-service experiences they want and expect, which helps your IT department strengthen its reputation as a relevant, service-oriented operation. And of course, effective self-service frees up IT resources, so your team can focus on more important, strategic projects.

**Experience the Advantages of “Single Pane of Glass” Workspace Management**

UEM should be much more than a family of loosely connected endpoint management and security products. Instead, it needs to be a tightly integrated set of tools that work together to simplify, streamline, and automate every part of your workspace infrastructure.

**Complete Self-Service with UEM**

Take advantage of a complete range of self-service capabilities built into UEM:

- **ITSM**: Access to an intuitive service catalog from any device
- **Mobile Management**: Device tracking and separate containers for corporate and BYOD resources
- **Desktop Containerization**: Convenient eStore experience for instant access to desktop containers

**Experience the Advantages of “Single Pane of Glass” Workspace Management**

UEM should be much more than a family of loosely connected endpoint management and security products. Instead, it needs to be a tightly integrated set of tools that work together to simplify, streamline, and automate every part of your workspace infrastructure.

**More Freedom through Better Security**

Every organization wrestles with the inherent tension between providing users with the easy, flexible access they want—and keeping information and assets secure and compliant. UEM should help resolve this tension through sophisticated security capabilities, so you can
expand access to resources, apps, and information beyond the walls of your organization without putting your business at risk. This should include:

- **Complete, automated patch management** that monitors patch compliance on all your Windows and Linux endpoints, quickly identifies and assesses vulnerabilities, and applies updates to keep all your endpoints patched and secure.

- **Full disk encryption** that protects every bit, byte, and file on every PC in your organization, so you can stop worrying about security breaches and data loss.

- **Policy-based data encryption** that creates “safe harbor” encrypted folders on your PCs and fully encrypts removable storage devices.

- **Wi-Fi management and security controls** that allow you to create white and black lists for wireless access points, enforce policies that restrict or block Wi-Fi communications based on set security or encryption standards, and more.

- **USB and storage device security** that allows you to enable, disable, and set access rights for removable storage devices, provides granular white listing controls for USB devices, prevents unauditabale transactions on local storage devices, and more.

- **Advanced firewall protection** that provides Network Driver Interface Specification (NDIS) level security for network traffic the moment it enters one of your PCs.

- **Policy-based application control** that blocks known malicious applications, controls access to applications based on a user’s location, and ensures that the proper security applications are running on your endpoints.

- **A complete mobile security solution** that enforces proper password usage and encryption on mobile devices, makes it easy for users to remote wipe or disable lost or stolen devices, provides detailed security reporting, and more.

- **A secure desktop containerization solution** that packages all of the files, settings, runtimes, and components applications need to run in one secure and protected container.

- **Mobile application management** that provides IT the ability to manage enterprise apps and data on an end-user device, without compromising end-user privacy

With UEM, all of these security capabilities should work together to help you to extend the boundaries of your security perimeter, grant appropriate safe access to any device, and ultimately keep your users and information safe in any workspace environment—whether it’s a wired PC in a cubicle at your corporate headquarters or a tablet accessing a public Wi-Fi connection at the airport.

**Stay Compliant in Any Workspace**
Compliance can quickly become a major challenge as you work to support the ever-expanding variety of devices, apps, locations, and connections that make up today’s workspaces. As your environments inevitably become more diverse and complex—and as your users become more sophisticated and independent—tracking, enforcing, and documenting compliance can start to feel like an overwhelming task.

UEM approaches workspace compliance in much the same way it approaches workspace security—with built-in key features and capabilities. This creates a complete, integrated compliance framework that’s capable of accommodating and supporting all of today’s workspace environments.

Compliance starts with a proven asset management foundation for all of your traditional endpoints. With some of the industry’s most advanced asset discovery, inventory, auto license reconciliation, license compliance, and reporting capabilities, software asset management (SAM) should give you everything you need to eliminate license over- and under-purchasing, avoid costly licensing penalties, and comply with license agreements and regulations.

Next, endpoint security management, full disk encryption, and patch management should include the sophisticated tracking, enforcement, and reporting capabilities you need to maintain and prove corporate security and patch compliance across all of your endpoints.

And finally, mobile management extends these asset and security tracking and management capabilities to all of your mobile devices—including both corporate and privately owned devices. With mobile management, you should be able to accurately track licensing and usage on any mobile device, so you can always know and document what you have, what’s being used, and how many you need to pay no matter how many different apps or BYOD devices you’re dealing with.

Together, these compliance capabilities make sure you always have the tracking, enforcement, analysis, and remediation tools you need to keep all of your workspaces compliant—no matter how unconventional or diverse they become.

**Start Enabling Your Secure, Compliant, and User-Centric Workspaces Today**
As modern workspaces continue to evolve, a few things are clear. Workers will continue to become even more dependent on an even wider range of mobile devices. The boundaries between work and personal will continue to
disappear. And the expectations of being able to get work done from any location, using any device or service, over any wired or wireless connection will continue to grow.

To succeed and thrive in this reality, IT organizations need better, more aggressive tools that support and enable today’s diverse workspaces. UEM should embrace this challenge, with solutions that extend the exceptional experiences and access users want—and the security, compliance, and control businesses require—to any workspace environment.