Orchestrating Digital Workspaces: Step-by-Step Guide to Making the Vision a Reality

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
March 2018

Prepared for:

ivanti

EMA™

IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Transforming End User Computing with Digital Workspaces

Expanding requirements for workforce mobility, heterogeneous device support, and distributed software ecosystems have challenged organizations to deliver secure and reliable IT resources (including applications, data, email, and other technology services). IT managers are finding it increasingly difficult to satisfy the unprecedented demands of their supported users for easy and unfettered access to business software and information from any device at any location at any time. Traditional endpoint management processes (which were principally designed to support a single operating system, Windows)—are unable to keep up with the rapidly evolving requirements for enabling a "digital transformation" of how end users interact with business technology. As a result, many organizations are finding they are unable to achieve required levels of security, reliability, and end user productivity.

To empower todays more technology-reliant workforces, organizations must transition from traditional distributed desktop environments to consolidate service delivery solution that establish a common use work environment across all devices they employ to perform job tasks. These "digital workspaces" enable standardized business work environments that are fully customizable, easy to maintain, and eminently secure. Adopting a digital workspace approach to endpoint management enables users to self-manage their work environment in a way that reflects their own personal preferences without having to constantly contact help-desk support. Additionally, digital workspace solutions substantially reduce administrative efforts and related costs while improving IT service reliability and security.

Unfortunately, decades of supporting distributed PC desktop environments has left most organizations reliant on antiquated management tools and practices that actually inhibit business performance in an age dependent on heterogeneous endpoints and distributed software ecosystems. Organizations are just starting to recognize the value of adopting a digital workspace approach, and those that do are initially faced with a critical question—where to begin? There are so many individual components to endpoint management practices that a transition of this magnitude can seem overwhelming to IT managers already overburdened with complex, day-do-day support requirements.

To help organizations determine the optimal processes for migrating distributed desktop environments to more pragmatic digital workspaces, EMA conducted primary, survey-based research on the end user experiences and IT management practices from organizations across a wide variety of business sizes and industries. The resulting statistical data, along with best practices identified in the Information Technology Infrastructure Library (ITIL), was used to develop a step-by-step transition process. The EMA Maturity Model for Digital Workspaces is segmented into five management phases (Figure 1). Each phase is comprised of a series of management improvement steps that should be introduced before moving to the next transition phase. Not all steps in each phase will apply to every organization, so some customization of this process may be necessary to adapt it to each company's unique business requirements.

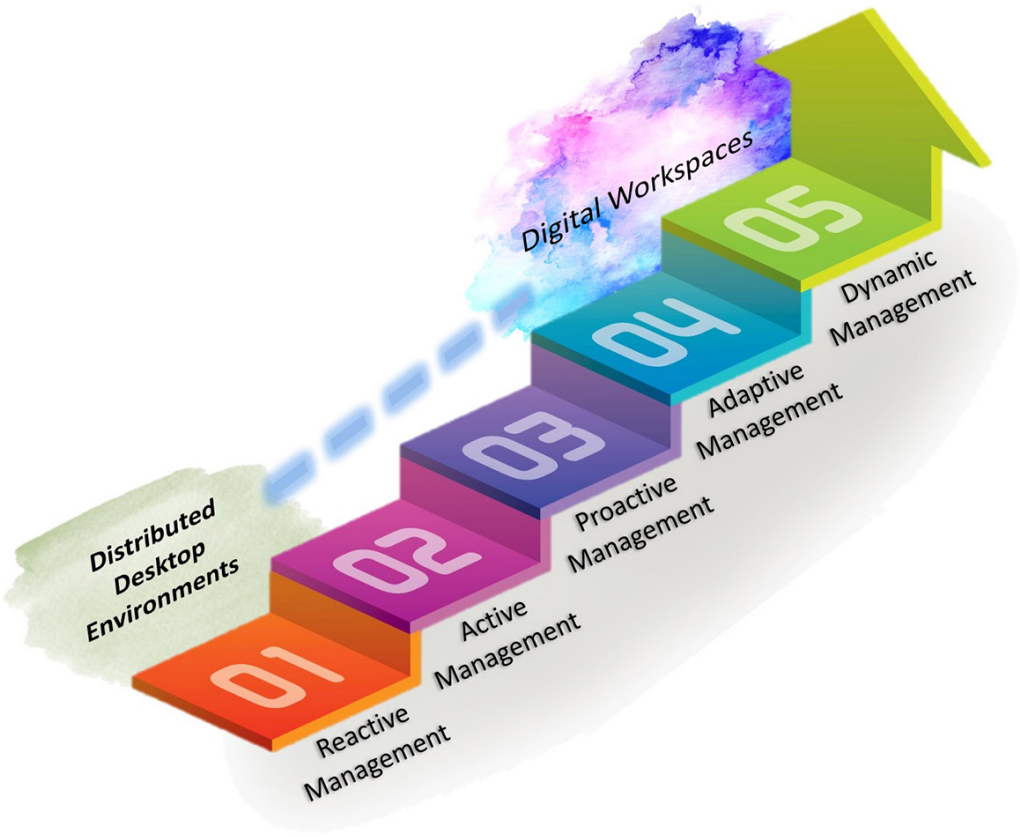

Figure 1: Management phases for the EMA Digital Workspaces Maturity Model

Here is a brief description of each management phase for orchestrating digital workspaces:

- **Phase 1: Reactive Management** – For many organizations, this phase represents the starting point. Little, if any, actual endpoint management is provided by the company and end users are mostly left to install and support their own devices. Applications may be purchased by the company, but they are either pre-installed at the time the device is purchased or downloaded by the end user from a public app store. Endpoint security is limited to just native OS security tools and, at most, a basic malware protection package.
- **Phase 2: Active Management** – The primary focus of this phase is on laying the foundation for endpoint management and establishing holistic visibility of the support stack. A unified endpoint management platform should be adopted that includes comprehensive asset data collection and inventory capabilities. Endpoint devices should be scanned for security risks and disabled from accessing business resources if determined to be non-compliant. Standardized environments should be established for hosting business applications and data.
- **Phase 3: Proactive Management** – At this phase, automated, business-dedicated processes are introduced for software and patch deployment as well as resource isolation to support BYOD requirements. Security management processes begin focusing on the prevention of breaches, rather than just the disablement of user access on detection of a breach. Impact of business practices on end user productivity is reduced and data sharing tools are introduced.

- **Phase 4: Adaptive Management** – The consolidation of management services and enabling user-focused customization of work environments comprise the principal emphases for this phase. Centralized support and security is enabled for virtual, web, and cloud-hosted resources. User self-service portals allow users to customize a common environment available on all devices they use to perform job tasks. With the successful introduction of all process in the Adaptive Management phase, organizations have achieved the delivery of digital workspaces.
- **Phase 5: Dynamic Management** – The optimization of digital workspace environments through automated management processes comprise the key elements of this phase. User policies are context-aware, app delivery is enhanced to meet usage patterns, and analytical security policies identify both known and unknown risks. Extensible automation is employed at this phase to streamline the delivery of software services and enhance user-focused self-service capabilities.

To begin, organizations should identify where their organization currently resides in the maturity model. It is possible the business may have adopted management practices from several different phases. If so, start with the lowest phase that includes any step(s) not currently introduced in your environment. The EMA Digital Workspaces Maturity Model was designed to introduce the process improvements that will provide the greatest value to the business as soon as possible, so it is essential to complete the phases in numerical order. In this way, business productivity and security improvements will become evident even before full digital workspace environments are introduced. These successes will help justify executive buy-in to support the adoption of additional management improvements necessary to move up the maturity chart.

It is important to remember not to try and adopt multiple steps in a management phase at one time. Doing so can be risky, as it may not be easy to determine which process change is responsible for any unexpected performance problems that may occur. Instead, organizations should introduce process improvements systematically and allow “settle-in” time between steps to resolve any issues that may arise. Once the production environment is in a predictable and stable state, organizations can introduce the next step in the management phase.

Detailed below are the key management process improvements that need to be introduced from the Active Management through Dynamic Management phases. Since Reactive Management is effectively an unmanaged distributed desktop environment, it does not include process improvements and does not require detailed descriptions. Individual steps within each phase are logically organized into four categories: unified endpoint management, application management, security management, and user productivity management. Steps within each phase do not need to be performed in any particular order except where there are obvious functional dependencies.

Active Management

Unified Endpoint Management

All management processes necessary to support a digital workspace environment rely on the availability of a centralized console designed to monitor, manage, and secure all endpoint devices in the support stack. It is important at this early phase to ensure the adopted management platform supports both PC and mobile endpoints, since transitioning to a unified platform will be much more difficult at later phases of the maturity model when dependencies have already been established for critical management services. If independent management platforms have already been adopted, the initial step should be to examine both platforms and determine if one of them can take over for providing primary support to all endpoint devices. Alternatively, if multiple platforms have been adopted and neither provides sufficient heterogeneous support, management processes should be migrated to a true unified endpoint management platform before any additional service improvements are initiated.

The adopted unified endpoint management platform should collect detailed software and hardware asset information for all supported devices and store them in a centralized data repository. Key data to collect should include device type, device user, device owner (i.e., company-owned or employee-owned), operating system version, patch levels, hardware configurations (e.g., processor, memory, storage, etc.), attached peripherals, key configuration settings, and both system and network performance status. A common reporting engine should be able to access the collected data and analytics should be provided to correlate conditions and events to simplify root cause analysis. Integration with listing services, such as Active Directory, will link established user and group information to asset owners.

At this phase, a formal help desk (i.e., level 1 support) should be in place to field user requests for problem remediation and to enable access to business services. IT administrators should be able to remotely access and control user devices to assist with installations and to repair any functional or performance issues. All user reported incidents and administer activities should be recorded in an incident management or help desk ticketing system. Ideally, this system will directly integrate with the unified endpoint management platform to link asset and status information in order to simplify endpoint identification and eliminate the need for administrators to input asset details into the incident ticket.

Application Management

All business-related applications, application patches, application configuration settings, and software license information should be collected from supported devices and stored in the centralized data repository on the unified endpoint management platform. Reports should be generated on existing application installations to ensure they are appropriately licensed and configured to meet enterprise compliance requirements. Endpoints should also be monitored to ensure they continuously meet established requirements and alerts should be sent to IT administrators warning of any out-of-compliance devices.

Any applications that are supplied by the business and downloaded to end user devices should be hosted on a centralized platform, such as an application server or private cloud. This will establish a single environment that IT administrators will need to support and secure. Additionally, locally hosting application services ensures businesses maintain control over their software assets, and distribution/installation processes can minimize impacts on network performance. For instance, rather than have each employee download an application update directly from a software vendor and taxing connectivity to the Internet, a single copy of the application update can be cashed on the centralized software repository and then locally distributed to the endpoints. Applications that are hosted in the centralized repository should be made accessible through a user self-service portal, such as a business-dedicated app store. This portal should be accessible from any endpoint device and should automatically present available software packages applicable to its operating environment (e.g., Windows, Mac, iOS, Android, etc.).

Security Management

Device-level security should be enabled on any endpoint used to access business applications, data, and services. This includes the automated scanning and remediation of malware, including viruses, spyware, adware, and Trojan Horses. The results and status of these scans should be centrally collected and alerts should be sent to IT administrators on detection of malware or if periodic scans are not regularly completed. Access to business resources from any compromised devices should be automatically disabled until the malware is removed or scans complete successfully. Mobile devices should also be monitored to determine if they are rooted or jailbroken to circumvent business security requirements, and PC configurations should be examined to ensure they have properly secured network ports, libraries, and registry settings.

Any device that accesses company data should be able to be remotely locked or wiped to prevent unauthorized access in the event the device is lost or stolen. While this functionality is commonly offered with mobile device management platforms, similar capabilities should also be provided to support PCs (particularly laptops, which are also portable and easily stolen devices).

Identity and access management processes should be employed to ensure data loss prevention. Employ robust multi-factor authentication before granting access to enterprise data, and record all access events (i.e., who accessed what and when) to provide forensic information in the event of a data breach. Access records can also be used to provide proof of compliance to meet regulatory commitments. End users should also be provided with easy-to-use methods for secure data sharing. This could take the form of a centralized data repository that appears as a mounted share or a data delivery system that is only accessible by authorized personnel.

User Productivity Management

Organizations should standardize on a common suite of business productivity applications, such as Microsoft Office or Google Docs. User preferences should play a critical role in determining which packages will be offered, but having a fixed set of supported applications will reduce the number of support variables for enabling security, patching, and software distribution. All approved applications should be offered in the enterprise app store or other self-service user portal. It is also advisable that the same productivity apps be provided for all supported endpoint types. For instance, if employees regularly use Office 365 on their Windows laptops, access to Office 365 should also be offered for their iOS tablets.

Companies should also provide a business-dedicated email system that allows users to easily send messages and data to approved colleagues but restricts the distribution of company information outside of the business network. It is essential that both the email system and any business-supported data sharing solutions be intuitive and friendly to employ so that end users are not tempted to use unapproved methods for distributing potentially sensitive company information. Similarly, business-dedicated messaging and/or texting tools should be provided that enable secure communications and data sharing.

Proactive Management

Unified Endpoint Management

Any endpoint devices that are permitted to be used for non-business purposes must logically isolate enterprise applications, data, and services with BYOD management practices. There are a number of methods available to achieve this. For mobile devices, organizations can adopt workspace containers, individual application containers, or app wrapping. EMA primary research indicates users are slightly more productive with individually wrapped or containerized applications because these do not require them to switch back and forth between duel persona environments.[1] However, the same research results indicated that workspace containers are easier to manage and secure. On laptop and desktop PCs, the most common method for enabling resource isolation is to employ desktop or application virtualization. A digital workspace approach may employ any or all of these approaches or may simply flag individual software elements as business resources. Regardless of which solutions are employed, it is essential that all application management tasks be performed directly from the centralized unified endpoint management console.

By this phase, all security management practices should be directly integrated with the unified endpoint management solution. This will allow condition-based automation to initiate security procedures offered by third-party providers. Additionally, security events and status data should all be recorded in the centralized data repository so a single reporting and alarming engine can be employed to correlate events and rapidly identify out-of-compliant endpoints. Also, security patches, system patches, and software update processes should all be fully automated and commonly performed by the unified endpoint management platform. Software update packages for all supported endpoint platforms should be staged on a business-hosted server and automated processes should ensure the prompt installation of patches on all supported endpoints.

Application Management

The enterprise App Store or user application access portal should be expanded to include support for any web-accessible applications. This can appear as a simple link that initiates a secure web browser session, but all access and authentication processes should be governed by profiles defined on the centralized management system. Similarly, software-as-a-service (SaaS) apps that require downloadable access software should be made available in the business-dedicated App Store or user portal and centrally secured and governed. Application patches and updates from third-party vendors should also be offered through the distribution service or automatically installed on endpoints as part of the system and security update processes. If the organization hosts any virtual applications, management services for provisioning these should be directly integrated with the centralized unified endpoint management platform, and users should have the ability to request access to these directly from the distribution service. From an end user perspective, all of these application types (web apps, SaaS apps, and virtual apps) should appear in the App Store or access portal as any other downloadable app.

Since end users frequently change, update, or add devices, application migration processes should be introduced that automatically map installed business apps in existing devices to equivalent apps in new devices. Compatibility and dependency mapping features should be included to ensure any software migrated to the new device functions correctly. This will substantially minimize challenges for existing users to onboard any additional or replacement devices and will quickly get them back to performing job tasks.

[1] "Effective BYOD Management: Empowering a Mobile Workforce," May 2016

Security Management

Policies defined in the centralized unified endpoint management platform should define which software elements are approved for use on business-used devices or containers (white listing) and/or should explicitly restrict access to software that is not approved for business use (blacklisting). A virtual proprietary connection (VPN) or other secure network connection services should be provided to end users to safely allow remote access to business systems. Authentication processes for the secure connection service should also be governed by the centralized management platform. Moreover, an enterprise-dedicated web browser should be provided to end users to allow secure access to business-hosted web services.

Device tracking functionality should also be provided at this phase to help recover any lost or stolen devices. However, to ensure user privacy, users should have the ability to opt-into or activate this service, and no tracking should be performed by administrators without a user's consent. Additionally, all business data should be encrypted when at rest on the hosting environment, when in transit over the network to a user device (transport layer encryption), and when in active use on the endpoint. In this way, even if sensitive business files are compromised through a lost device or inappropriate distribution, individuals with malicious intent will be unable to access the data without the correct access key.

Security compliance audits should now be fully automated. Not only will this simplify the periodic process of needing to provide proof of compliance, but it will also enable the real-time identification of out-of-compliance devices, allowing them to be remediated before being flagged in an official audit. This continuous compliance approach has the added benefit of substantially reducing security risks by identifying potential problems before a breach occurs.

User Productivity Management

In order to minimize the impact of authentication practices on user productivity, single sign-on (SSO) functionality should be adopted. Ideally, the SSO solution will only require a single password to be entered to access all business services, including email, web services, virtual apps, SaaS apps, remote access, enterprise apps stores, data shares, and containerized resources. The data storage repository should also be enhanced with file synchronization capabilities to support user collaboration and multi-device use. In this way, data can be downloaded on multiple user devices and any changes made to the different copies will be automatically synchronized with the master version in the data repository. From a user perspective, the same files appear to be always available on all of their various devices or the devices of their peers.

Users should now have the ability to set their own privacy settings to prevent their employers from reviewing non-business-related activities (such as private web surfing). However, access to some services may be disabled if users choose to block access in environments that require enhanced security and compliance visibility. What is important is that users have the clear option to choose to allow business access to their devices in exchange for the ability to access business resources from them.

Adaptive Management

Unified Endpoint Management

All user and device profiles should be established and maintained within the centralized management console that defines all authentications, access rights, and configurations for business applications, data, and services. Profiles should be organized according to groups—for instance by user roles (e.g., sales managers, accountants, IT administrators, etc.), departments, device types, or any other common identifiers. This will allow the creation of master profiles that can be applied to all users with similar requirements. Through already-established integration with listing services (such as Active Directory), users can be preassigned to particular groups. When those users onboard a new device, the predetermined settings and software for that user's group can be automatically applied on the endpoint without the need for end user or administrator interaction. Further, administrators only need to maintain profiles for a limited set of groups, rather than all users in an organization. However, individual profiles within groups should be further customizable to support any unique user needs.

The provisioning of virtual desktops should be automated and access to virtual desktops should be enabled from the user self-service portal. This includes enabling access to all supported desktop virtualization platforms, including VDI, desktop-as-a-service (DaaS), terminal services, and/or client-hosted desktop virtualization. If applicable, the provisioning of hypervisors for all supported device operating environments should also be made available through the user self-service portal, and SSO support should be extended to virtual desktop sessions.

Application Management

At this phase, the enterprise apps store or application portal should be expanded into a full user self-service catalog that provides a "one-stop shopping" experience for end users to access all business services. In addition to providing access to downloadable and remote applications, the service catalog should enable access to data storage resources and any automated business management systems such as for timecards, schedulers, change management, purchasing requests, or to initiate IT service requests. A facility should also be included that allows users to request new apps or service to be added to the catalog or to request authorization for accessing resources that were not previously approved for their use. All user requests should be automatically forwarded to the appropriate management personnel for review.

The entire software ecosystem supporting business services, including both internal and external resources, should be mapped to identify dependencies and relationships of software components. This is particularly true for software subsystems that operate independent of an application. For instance, a software tool may need to call a remote database to acquire information essential to completing a particular task. The performance of that tool, therefore, is contingent both on the application itself and the availability of the remote database. In the case of hybrid applications, a number of these types of software subsystems may be distributed across both internal and external hosting environments, and the relationships between these must be clearly identified. Problem identification and resolution are greatly simplified when administrators can easily identify all software components relevant to an application process and correlate these to the underlying network and hardware infrastructure components supporting them. Additionally, a visual or otherwise easily understandable map of the software ecosystem will provide the critical intelligence necessary for making performance improvements to application services.

Security Management

While passwords continue to be employed as the most popular method of authentication, it must be recognized that passwords also represent the weakest link in risk mitigation. End users often set weak passwords, use the same passwords for multiple services, and rarely change passwords unless prompted to do so. Some users have even been known to write down there passwords in locations that are easily detectable by potentially malicious individuals. By this phase, automated password enforcement processes should be adopted in conjunction with the previously introduced SSO capabilities. Users should be regularly prompted to update access credentials with strong passwords, and automated password recovery tools should be introduced that allow users to recover their access in the event they forget a password. However, since this approach to authentication is known to impact user productivity, it is recommended that alternative methods of authentication—such as device authentication or biometric authentication (i.e., fingerprinting, retinal scans, or facial recognition)—be employed on devices where such resources are available.

Security management practices should be directly integrated with network management platforms. This will allow security solutions to dynamically establish secure network connections (such as SSL VPNs) to remote endpoints and enable application-level monitoring of network transactions that may be sending or receiving inappropriate data, such as a virus or other types of malware. Network traffic data can also be analytically examined to identify potential attacks or security breaches that would not otherwise be visible to administrators only reviewing system- and application-level conditions and activities.

User Productivity Management

The user self-service catalog should now only present services applicable to the user and device accessing them. As the catalog grows over time, application sprawl can make it more difficult for users to identify the particular software they require. This inconvenience can be significantly reduced by not displaying any resources that would not be applicable to the user accessing the catalog. Additionally, the catalog should be logically organized to more easily identify software elements, and a search engine should be included to help identify applications based on characteristic tags rather than just package names.

New business-dedicated resources should be introduced to facilitate user collaboration and communication, such as tools for video conferencing, contract signing, desktop sharing, and white boarding. The centralized security and unified endpoint management system should govern these services, with access and authentication privileges defined in the common user profiles. Event scheduling should be enabled either directly from the endpoint or through a feature in the service catalog.

Dynamic Management

Unified Endpoint Management

Up to this point, all policies established in user profiles were static rules. For instance, only accountants may have access to the company edition of QuickBooks. However, to ensure proper security and compliance attainment, a much more complex set of rules that are context-aware may need to be adopted. For example, only accountants may have access to the company edition of QuickBooks IF they are connecting to it while physically in the office facilities and IF they are not actively running any desktop-sharing software. Context-aware rules can be placed on changing states, such as the types of applications being used or if the user is performing any suspicious activities.

The example above references a context-aware rule set called "geofencing," which places usage restrictions based on the physical location of a device. However, it is important to remember that geofencing should always be used in conjunction with network fencing (restricting access based on the type of network connection). While a particular user may be physically on-premises at their office, they could still be connecting to business resources over a public cellular network, which is inherently unsecure. Conversely, off-premises users (for instance, sitting at the local coffee shop) may be using a VPN connection to access business resources, which would make them appear on the local business network even though they are physically at an unsecure location. Only by creating rules around both network and physical locations can risks of exposure to users be truly moderated.

Application Management

The performance of all essential enterprise applications should now be monitored on endpoints to ensure they are continually functioning within expected parameters. Historical trending of application performance will help identify slowly degrading services and can alert IT operations to problems that they can repair before they impact the workforce. Similarly, software usage patterns should be monitored to proactively manage application availability. Server and license capacities may need to be increased for heavily used software, and the identification of unused applications will provide opportunities to reduce operational costs by eliminating or repurposing software licenses. In some cases, software metering may be employed to restrict the number of users that can use a particular application at any given time. Software metering can be built directly into individual applications or operate as a function of the software catalog.

In the event application performance or availability drops below predetermined thresholds, automated processes should adjust service delivery conditions to dynamically return the performance to an acceptable state. Principally, this is accomplished through integration with workload automation and a software-defined data center (SDDC). For instance, a software service experiencing issues may be automatically moved to another server, have additional instances activated, have its storage capacity increased, activate additional CPUs for better load balancing, have network traffic rerouted to low-use segments, or throttle other low-priority processes that may be interfering with service performance (such as backup or mirroring processes). In this way, application services are continuously kept at peak performance with little or no administrator interaction, and IT impacts to user productivities are minimal or nonexistent.

Security Management

Vulnerability assessments should be performed in real-time to immediately identify any security breaches or potential threats to supported endpoint devices, business networks, and application-hosting environments. While security policies were previously based on predefined conditions, analytics should now be applied to address security threats that were not previously identified. For example, if an application accesses or transmits data to an external system, a risk assessment should automatically be performed to determine if the activity could be considered a threat and blocked. This analytical threat assessment will allow organizations to rapidly identify unknown threats in addition to already-identified threats. Further, this approach prevents "zero day attacks" since it does not rely on the deployment of patches or configuration changes to secure the environment.

Recognizing that not all data needs to be protected with the same level of security, organizations should adopt data protection solutions that automatically flag confidential or sensitive information based on key words in the content or other distinguishing characteristics. More stringent policies can then be applied to flagged data to limit its accessibility and distribution. Compliance monitoring processes should also be enhanced with automation to enforce security practices and return out-of-compliance systems to a state that meets business requirements. Any endpoint devices that cannot be governed by continuous compliance services (such as employee-owned devices) should be disallowed access to any remote business resources or to any business data or application currently residing on those devices until the threat is mitigated.

User Productivity Management

Up to this point, automation was used to support common tasks applicable to a broad range of users. More personalized and customizable automation should now be introduced to support repetitive user tasks that are not addressed by existing applications. For instance, process automation can be employed to achieve complex document approvals or product evaluation tasks by handling all the distribution and record-keeping tasks that would otherwise need to be performed by the workers. These specialized tasks may only be applicable to one or a few employees, but can have a profound effect on reducing their workload. To prevent IT operations from taking on the burden of scripting or coding solutions for all user activities, an automation platform should be adopted that is accessible to all end users through the self-service catalog. The platform should be intuitive to use, with drag-and-drop widgets and visual process flows, so that users can create their own customized automated solutions that will address their unique job requirements and accelerate their productivity.

DIGITAL WORKSPACES

	REACTIVE MANAGEMENT	ACTIVE MANAGEMENT	PROACTIVE MANAGEMENT	ADAPTIVE MANAGEMENT	DYNAMIC MANAGEMENT

UNIFIED ENDPOINT MANAGEMENT	• Remote desktops and devices principally installed and maintained by end users	• Unify PC and mobile management on a single console
		• Integrate listing services
		• Employ a common reporting engine for all endpoints
		• Provide remote device support
		• Consolidate asset and inventory management
			• Isolate business resources with BYOD management practices and solutions
			• Automate system patching and updating processes
			• Integrate security management with endpoint management
				• Consolidate profiles onto a single management interface
				• User profiles
				  • Device profiles
				  • Security profiles
				• Automate virtual desktop provisioning and management
					• Enable context-aware policies and profiles
					• Employ geofencing in conjunction with network fencing

APPLICATION MANAGEMENT	• All applications are locally installed on remote devices	• Track installed enterprise applications and licenses
		• Host downloadable business software on a centralized platform
		• Establish an enterprise App Store to enable access to business software
			• Incorporate web apps and SaaS apps into App Store
			• Automate application patch and updating processes
			• Automate virtual application provisioning and management
			• Automate app migration processes
				• Expand business app store into a full user self-service catalog
				  • Include access to data repositories
				• Map software ecosystem (including app subsystems)
				• Enable support for hybrid apps
					• Monitor app performance and software usage patterns
					• Meter software usage
					• Automatically adjust IT service delivery to address end user performance issues and requirements
					  • Integrate with SDDC

SECURITY MANAGEMENT	• Native OS security features only (with default settings)	• Detect rooted and jailbroken devices
		• Scan for and remediate malware
		• Enable lock and wipe of business resources on non-compliant endpoints
		• Protect business resources with identity and access management
		• Enable secure data sharing
			• Employ end-to-end data encryption
			• White and black list apps
			• Provide a VPN for remote access
			• Allow users to opt into device tracking
			• Enable secure web surfing
			• Automate compliance audits
				• Adopt non-password-based authentication processes
				  • Device authentication
				  • Biometric authentication
				• Integrate security management with network management
					• Perform real-time vulnerability assessments
					• Analytical security policies identify both known and unknown risks
					• Identify confidential/sensitive data
					• Automate real-time continuous compliance

USER PRODUCTIVITY MANAGEMENT	• None	• Standardize business productivity tools • Provide dedicated enterprise email • Provide dedicated enterprise data repository • Provide business-dedicated messaging/texting tools	• Enable single sign-on features to minimize security impacts on user productivity • Allow users to select privacy settings • Enhance data storage with file synchronization	• User self-service catalog should automatically adjust to present appropriate service for user roles, requirements, and devices • Provide business-hosted communications and collaboration tools	• Employ automation to enhance self-service capabilities

Figure 2: EMA Digital Workspaces Maturity Model

EMA Perspective

The EMA Digital Workspaces Maturity Model was intentionally developed to spell-out all the key processes that must be introduced at each transition phase. However, a casual reader may interpret this as providing a complex series of requirements that would be extremely challenging to implement. Indeed, this may actually be the case if an organization decided to adopt independent tools to support each process improvement. While organization can see some initial improvements from the adoption of point products that provide support for only one or a few process requirements, over time unintegrated products become costly to maintain and difficult to manage. Ultimately, point product sprawl will substantially increase the complexity of endpoint management practices with the need to employ multiple interfaces to support a common set of devices. This "swivel chair management" approach is not only time-consuming, but also makes it nearly impossible to correlate conditions and events across the various tool sets. As a result, organizations that principally employ point products are rarely able to enable the holistic visibility and automation necessary for them to move beyond reactive IT management.

EMA advocates the employment of comprehensive management solutions that are both modular and integrated. A modular solution allows organizations to adopt the management resources as they are required for each transition phase. Additional resources can then be adopted when the business is ready to move up the maturity chart and as budgets become available. However, to prevent point product sprawl, it is essential that all components of the management platform be fully integrated to create a seamless management experience from a common console interface. The processes outlined in the EMA Digital Workspaces Maturity Chart indicate the key functionality to look for in any solution that will be evaluated. A modular and integrated endpoint management platform that addresses the breadth of digital workplace requirements allows organizations to focus on effectively conducting the transition process rather than stressing over how to deploy each individual administrative tool.

Additional Reading…

For more information on orchestrating digital workspaces, please see EMA's other white papers in this series:

"Orchestrating Digital Workspaces: The Emerging Digital Transformation"

"Orchestrating Digital Workspaces: The Evolving State of Endpoint Management"

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3674.020818