Converged management: data, devices and user

March 2019
Table of contents

Executive summary 3
Device life cycle – Endpoint as a Service 3
End-user mission management objectives 5
OS release train considerations 5
What are the management options 7
What’s next? 10
Executive summary

The modern digital workplace requires data and artifact access that is seamless, secure, collaborative and productive. The enterprise artifact access must work so users are productive. Endpoints and devices have expanded beyond the enterprise workstation comprising a PC or laptop but include mobile devices, tablets, Macs, Chromebooks, high definition video endpoints and many others. Organizations want the endpoint life cycles managed for all endpoint types with device life cycle and endpoint as a service (EaaS) solutions. They want all their endpoints managed seamlessly and the ability to scale up or down as necessary.

Client management for end-user compute devices has dominated the market for years, managing laptops and PCs as well as providing data loss prevention (DLP) and policy enforcement. When the market changed with the introduction of new endpoints such as smartphones and tablets, enterprise mobility management (EMM) was developed to manage DLP on smartphones, tablets and other mobile devices. These two different management schemes have been separate for many years. Users demand ubiquitous device options for the digital workplace while enterprises want productivity and DLP—blurring the line between traditional client management solutions with newer EMM solutions.

With converged management (CM), which unifies client management and EMM into a single solution and portal, all endpoints can now be managed from a single solution whether they are Windows, macOS, iOS, Android, laptops, desktops, smartphones, Chromebooks/Chrome OS, or any other device. DLP is paramount in today’s agencies and enforcing policy, security and governance across all devices for a given organization is now much easier and affordable with CM.

Device life cycle – endpoint as a service

Perspecta’s device life cycle – EaaS provides options for your agency and mission to shift from a Capex model to Opex or maintain a traditional Capex model, whichever fits your mission. This solution allows you to completely focus on your mission with services options to fit your needs. It avails a full life cycle of services with procurement, provisioning, including imaging and OS updates to align with OS release trains, application loading, converged management, expense management, asset management, help desk and the full support suite and break-fix, exchange, recycle and refresh.
The device life cycle – EaaS offering combines state-of-the-art devices (such as mobile, PC and powerful workstations) with value-added expertise in an all-inclusive managed solution under a single solution. By providing you with a single point of contact, device life cycle – EaaS allows you to scale up or down as needs warrant and significantly reduces the complexity and costs, both hidden and visible, of device procurement and deployment.

**Data security**

It's the data that matters, and that is why Perspecta provides secure solutions managing the data at the endpoint and access to that data using multi-factor authentication solutions. Perspecta’s device life cycle/endpoint as a service and converged management solutions create a secure environment allowing the user to access only the data necessary and when they need to on any device. If a device is lost or stolen, our solution provides encrypted containerized data protection along with the ability to remotely wipe the device. Additionally, we offer virtual desktop solutions where the data is never stored on the endpoint, meaning that if a device is lost, stolen or compromised, protections are in place to ensure the data is safe.

**Derived credential**

Digital IDs allow you to streamline the user experience while maintaining security using derived PIV credentials. This places a digital ID onto the device which maintains the same state as the PIV card itself. If the PIV card is suspended or revoked, the derived PIV credential also will not be able to access agency artifacts. With a derived PIV credential, the user accesses agency resources just as they would a PIV card itself, but with their device and not a PIV card plugged into it or plugged into an expensive SLED device.

**Scaling**

When you have a seasonal need or a demand for endpoint assets, our solution allows you to keep up with these by quickly supplying you with the resources with a quick turnaround. When you need more, you order more; and when the wave passes, the devices are scrubbed per your standards, recycle and repurposed.
End-user mission management objectives

Modern operating system (OS) development uses agile approaches and each OS vendor releases new versions of their software addressing integrity, security and new features in rapid release cadences. Each vendor is on a different release train, and each vendor’s OS’ integrity, security and new feature priorities may or may not align with your mission schedule. Some OSs were originally designed emphasizing enterprise requirements while others were designed with end-user focus—for example, hand-held mobile end-point OSs. In some cases, you have no choice but to adopt the OS release update over a specified period of time or forfeit supportability and integrations with your other mission-critical applications and data. All of these changes pose a management challenge and an increased security risk. As endpoints and OSs continue to evolve, you need a management solution that will address your full mission needs. CM removes the ambiguity from having separate management tools for different OSs and endpoints and provides a common endpoint management platform for mission governance, risk reduction and policy enforcement. CM also allows different policy, security and governance rules to be applied to different user groups, no matter the device makeup, or by device groups or a combination of both.

Here are some key questions to ask: What devices and user groups are in scope? Are servers also in scope such as Windows server? What endpoint OSs are in scope—such as iOS, macOS, Android, Windows 10, Chrome OS and Linux? Do you want the solution to rapidly evolve as the OSs, devices and servicing environments rapidly evolve? Do you want the management solutions on your premises or sourced from the cloud? Do you desire a common management console for all devices?

OS release train considerations

When implementing CM, there are certain OS release train update aspects to consider dependent on which OS a device employs. Each OS has different update methods and some are more flexible than others. OS release update methods are outlined below.

iOS release train

Apple has introduced controls from iOS 11.3 and later where enterprises can delay user OS updates for up to 90 days while they complete testing. Once testing is complete and enterprises allow the upgrade or the 90 day period expires, users are able to update their iOS devices. When you are ready, you can choose which iOS update version for users to download and install. You can push it to them directly.

macOS release train

In recent years and in most years, Apple releases a new version of macOS annually. Since the macOS High Sierra release, you can use the same management framework as you do for managing iOS devices. macOS management is supported in Microsoft Intune from OS X El Capitan 10.11 and later.

Android release train

Android releases can be controlled with Samsung Knox. However, Android releases outside of Knox are pushed out by carriers at their discretion.

Chrome OS release train

Chrome has three types of OS release channels: Stable, Beta and Dev. The stable release channel is the generally available current release. The Beta channel allows you to test the Chrome OS version four to six weeks
before Beta content moves to the Stable channel. The Dev channel allows you an even further head start on testing, however Dev is less stable and features are more likely to change. You can pick up Dev channel OS features nine to 12 weeks prior to when features arrive in the Stable channel.

**Windows 10 release train**

Microsoft gives you Windows 10 channel options that allow lead time and flexibility, while staying up to date. You do have a choice of how Windows 10 is updated. There are two Windows 10 channels: Semi-Annual Channel and Long Term Servicing Channel (LTSC) (including Windows Update for Business), along with an option to receive early versions before channel release with Windows Insider. You’ll have to determine which of these is best for your enterprise depending on the mission. See Figure 1 for how these servicing options are realized with increasing quality.

**Semi-Annual Channel**

Semi-Annual Channel was historically called Current Branch for Business. Semi-Annual Channel (targeted) used to be named Current Branch. These service options are easily pushed out and configured on the Windows 10 device and from Windows 10, version 1607 and beyond and feature updates can be delayed for up to 365 days. With Semi-Annual Channel new functionality is delivered twice per year. Upon release from Microsoft, feature updates are available immediately for targeted machines (Semi-Annual Channel-targeted). Each Semi-Annual Channel release is serviced for 30 months.

**Long Term Servicing Channel**

LTSC used to be named Long Term Service Branch (LTSB). LTSC is only available for Windows 10 Enterprise LTSB edition. It doesn't include many applications such as Microsoft Edge, Microsoft Store, Cortana, Microsoft Mail, Calendar, OneNote and Clock. LTSC is intended for appliance devices such as medical equipment, and point of sale machines—purpose-based devices that require a longer service period. LTSC provides only quality and security updates to appliances and prevents the LTSC devices from receiving normal Windows 10 feature updates. The quality and security updates can also be deferred, governed by a converged management solution. LTSC releases occur every two to three years and have a 10-year lifecycle.

**Windows Insider**

Allows you to get releases early before they are available in the Semi-Annual Channel. This allows you to get early visibility to feature updates. This pre-production release is available in this mode for testing and evaluation. Content is subject to change from Windows Insider to what ends up in the release of Semi-Annual Channel.
What are the management options?

When implementing CM, there are certain OS release train update aspects to consider dependent on which OS a device employs. Each OS has different update methods and some are more flexible than others. OS release update methods are outlined below.

**Microsoft Enterprise Mobility + Security**

Microsoft’s Enterprise Mobility + Security (EM+S) is a suite of integrated solutions comprising management solutions such as Intune and System Center Configuration Manager (SCCM), Identity, Cloud Access, Information Protection and Desktop Virtualization. For this document, we will focus on the management solutions Intune and SCCM.

**System Center Configuration Manager**

SCCM is an on-premise management solution using the traditional licensing model, which Microsoft continues to evolve. SCCM has robust deployment, management and reporting features and manages Windows PCs and servers, Apple macs and Linux servers. If you use SCCM today, you’ll have a robust solution for client and server management. There is a current option in use called Hybrid MDM, which is an integration of SCCM and Intune. Hybrid MDM is being deprecated and Microsoft is moving to Intune for all endpoint management. For servers, you will still need SCCM.
Intune
Intune is a CM cloud-only solution supporting iOS, Android, macOS and Windows devices as well as management of PCs, but it is not for servers. You’ll find it to be a quick and easy setup as it is a cloud subscription service with no on-premise equipment required. Intune is updated currently on a monthly basis, and the frequency is expected to increase. Intune is designed for robust management scenarios and scalable to very large mobile device deployments. Administration can be done anywhere from the web-based console. You’ll like the powerful management features and the ability to distribute apps to iOS, Android, macOS, and Windows targets including support for legacy windows installer apps.

What’s significant with EM+S?

Intune the converged management solution
Microsoft is moving to Intune in the cloud and away from on-premise or hybrid MDM solutions for CM. From Microsoft’s own case study, “As we move toward a cloud-only future and modern management, we’re working to streamline our physical infrastructure and reduce the overall number of traditionally managed clients to provide a modern workplace that’s always updated, always protected, and easily scalable.”

Intune for government
You’ll like that Intune continues to increase the number of government standards and certifications for compliance. Some of the more important presently complied with standards are: CJIS security policy, DoD DISA Level 2, Level 4, and Level 5; FedRAMP, FERPA, FIPS 140-2, IRS 1075, ITAR, NIST 800-171 and more. You can find Intune’s latest government compliance here: https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings?product=Intune

Microsoft Office productivity apps
The Microsoft office productivity apps such as Outlook, Excel, PowerPoint, Word and OneDrive historically could not fully be managed by third-party CM or EMM providers without Intune augmentation. Microsoft has exposed the Graph application programming interface (API) allowing third-party CM and EMM solutions to manage Microsoft productivity apps. This means that Intune is no longer needed in the same context to augment your CM or EMM solution, provided your solution has developed support for the Office productivity apps with the Graph APIs. In order to use the Graph APIs, you’ll still need all the end users to be covered under an Intune license which is usually part of your broader Office 365 and Azure AD enterprise agreement. Check your O365 or Azure AD enterprise agreement for details.

SCCM release train change and windows 10 management support
Like the Windows 10 rapid release channel, Microsoft placed SCCM on the release channel scheme to keep pace with Windows 10 changes. This includes Semi-Annual Channel and LTSC similar to Windows 10. Windows 10 has minor monthly releases, and semi-annual major releases. This means that you need to keep your SCCM environment current otherwise you run the risk of not being able to support Windows 10 releases and resolving potential security issues. This is a significant change to the management environment for most organizations.

Hybrid MDM is deprecated
As of August 14, 2018, Microsoft made the decision to announce the end of support for the hybrid MDM. On September 1, 2019, Microsoft will retire the hybrid MDM service offering. Hybrid MDM was the integration of Intune and SCCM for managing endpoints and servers. Microsoft made this announcement because Intune itself offers more features than hybrid MDM solution. You’ll have to plan for migration from Hybrid MDM to Intune. Microsoft has created a co-management option which you can concurrently manage Windows 10 devices using both Intune and SCCM to help manage the transition to Intune. Microsoft has provided a new migration process to move from hybrid MDM to standalone Intune converged management. This process has three steps: Microsoft Intune Data Importer, Mixed Authority and an Improved MDM Authority Switch. The Microsoft Intune Data Importer copies device management data created in SCCM to Intune automating the need to recreate all profiles, policies and apps. Mixed Authority selectively migrates users from the existing hybrid MDM to Intune in controlled phases. This is the transitory phase where you can migrate groups of users to Intune while other groups are still on SCCM. Next, once migration is completed and testing is completed, you’ll perform the MDM
Authority Switch. After this switch, all policies available in SCCM will be migrated to Intune. With this method, devices aren’t required to re-enroll. More details are found in Microsoft’s own case study: [https://www.microsoft.com/itshowcase/Article/Content/1042/Migrating-mobile-device-management-to-Intune-in-the-Azure-portal](https://www.microsoft.com/itshowcase/Article/Content/1042/Migrating-mobile-device-management-to-Intune-in-the-Azure-portal)

Windows app store
Microsoft has adopted modern app distribution using stores in addition to supporting traditional app distribution methods. The Microsoft store is for distributing your apps to anyone. You’ll use the Microsoft store for business as your own private store to distribute apps targeted to your enterprise. Your apps submitted to the Microsoft store are security, compliance and content tested prior to store publication. Additionally, apps submitted to your Microsoft store for business are under your control and can be made available to a few employees or to the entire enterprise, the choice is yours. Microsoft store for business is realized in the cloud so your employees will need Azure Active Directory (AD) accounts and they can self-enroll. You can distribute apps from the store or take the traditional Windows installer approach

VMWare Workspace ONE
VMware’s Workspace ONE is an industry leading CM solution managing most platforms of endpoints including virtualized endpoints, iOS, Android, Windows 10, ChromeOS and macOS. It securely delivers and manages any app on any device with integrated access control and application management preventing enterprise data loss at each layer. You’ll also appreciate the powerful conditional access feature where devices can gain access based on location or organizational role. With full biometric support and multi-factor authentication, your identity and authentication needs are supported. User adoption is paramount for success, and Workspace ONE drives rapid adoption of modern apps (SaaS and mobile) and legacy apps (native and web) from an optional personalized app catalog. You’ll have visibility across your entire organization to know the exact status of any endpoint or group of endpoints. One great feature is the ability to onboard an employee in under an hour with no staging—just hand them the device and Workspace ONE does the rest. You can also provision an employee anywhere in the world with a laptop out of the box in minutes. Depending on your mission needs, you can choose to run Workspace ONE from the cloud or on-premise, and you’ll have an architecture designed to work with all endpoints, even those not yet invented. Workspace ONE offers a per-user subscription rate for the cloud and on-premise versions.

What’s significant with Workspace ONE?

Integrations and scale
With Workspace ONE, there is a good chance it will integrate with systems and solutions you already have. In fact, there are more than 100 partner solution integrations in the Workspace ONE ecosystem covering all layers and applications categories from networking components to management and operations to productivity applications. You’ll also appreciate the administrative aspects of Workspace ONE, which allow you to segment Workspace ONE administration into different exclusive organizations within your agency with different administrators, all without having to use an additional Workspace ONE tenant. Your app development only needs to be done once with Workspace ONE as Workspace ONE is part of the AppConfig community ([https://appconfig.org/members/](https://appconfig.org/members/)). If you write your apps leveraging AppConfig’s common suite of APIs, then you can change to a different CM solution without changing your apps.

Location for your needs
Workspace ONE is offered as a service either from the FedRAMP moderate cloud or on premise. The choice is yours depending on your mission needs, with a subscription per user license covering multiple devices per user.

Workspace ONE for government
The Workspace ONE cloud is sourced from a FedRAMP moderate cloud and adheres to FIPS 140-2, NIST 800-53, NIAP (CSFC) Validation, CJIS and others, as it continues to grow its list of government compliance and certifications. You’ll also like using your device with a digital common access card (CAC)/Personal Identity Verification (PIV) derived credential with Workspace ONE’s integration with DISA PureBred and commercial derived credential solutions such as Intercede, Entrust and Xtec.
Easy migration to Windows 10 converged management
Workspace ONE eases the migration from Microsoft’s SCCM using the AirLift connector. The AirLift connector allows co-management as well as easy Windows 10 endpoint configuration data migration from Microsoft’s SCCM during transformation. This allows transformation to a cost-efficient CM solution to occur at your pace. Now that Microsoft has exposed the Graph APIs, Workspace ONE can now manage Office 365 productivity apps. To use the aforementioned Graph APIs, you’ll still need all the end users to be covered under an Intune license, which is usually covered under an Office 365 or Azure AD enterprise agreement. Check your agreement for details.

What’s next?

Now that you have an understanding device life cycle – EaaS options along with data and user governance with CM and OS releases, you can choose how you want your devices and the data on them protected and managed. With the CM and the OS release train update considerations, there are a few steps to take next on your path to fully optimized endpoint management and device procurement. First: determine the scope of endpoints requiring procurement and management. Next: determine the desired endpoint consumption model and available servicing periods available for each OS. For example, choose your Windows 10 servicing option, and for most applications except the most mission critical, the choice is Semi-Annual Channel. For mission critical endeavors that require extra scrutiny and less frequent change, choose LTSC. If in doubt, or if you have a unique situation, we can help you sort through the details.

Your device life cycle – EaaS needs can be met by our options and we will work with you for what is best for your agency. Your decision to transition to CM is significant but shouldn’t be difficult. It is not a question of if but a matter of planning when. You have to evaluate your current state and desired end state, including types of OSs and devices to be managed, security and DLP requirements, governance and policies, management requirements and timeline, and then choose the right path forward.

Perspecta recommends staying focused on your end-user endpoint needs, your end-user mission management objective, device pool size, required management features and weighing the benefits, complexities and risks in your decision. This paper discusses device life cycle – EaaS and the top two converged management leaders in this space to give you insight into what options are available to you. You’ll have to weigh your endpoint and device management solution deployment process timelines against product and service trends. These choices require guidance from a trusted advisor who can help you navigate through these options to transform your endpoint device life cycle, endpoint/PC and server management workloads.

Perspecta can help. Learn more at perspecta.com.
Author

Ed Wilmes
Chief enterprise architect, Digital workplace

Ed Wilmes has been contributing in various digital workplace, mobility, communications, security and cloud solution roles for more than 29 years and currently serves as chief enterprise architect for Perspecta’s digital workplace portfolio. Holding both master’s and bachelor’s degrees in electrical engineering, Wilmes has two patents granted and other patents pending. He has presented published research at IEEE, HP Discover and Enterprise Connect conferences and was a panelist speaker at the Smart Card Alliance conference in 2015.

Wilmes is an Open Group-certified master architect and an Open Group Master Architect Review Board member using his expertise to mentor and certify other architects. In addition, Wilmes is a PMI-certified project management professional. Throughout his career, Wilmes has brought to market various advanced technology products, which won Internet Telephony’s Product of the Year award. Additionally, he developed wireless technology in a successful venture funded startup that became T-Mobile.