Better user experience for IT admins

Comprehensive management of devices, apps, Windows 10, and security

35% less time to complete a mobility management solution setup scenario

Simplify digital workspace management for admins

VMware Workspace ONE created a better experience for feature-rich management than Microsoft EM+S

Each device in your company's infrastructure brings a digital workspace that needs security and management. With Windows® 10, macOS®, Android™, and iOS devices, this can require a hefty amount of an IT admin's attention. A streamlined enterprise management platform with robust options can help your admins understand complex processes easily and finish tasks quickly.

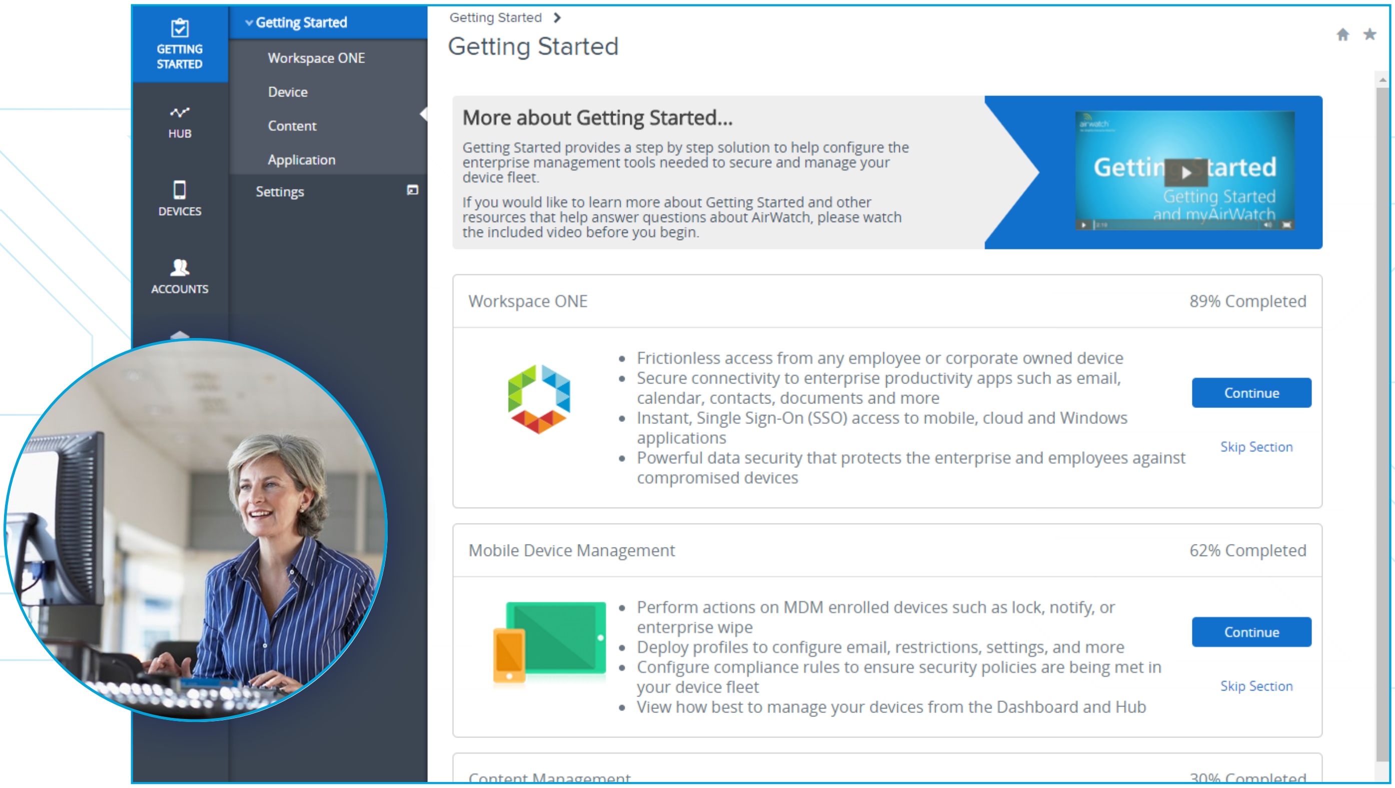
At Principled Technologies, we tested and studied a pair of platforms: VMware Workspace ONE™ powered by VMware AirWatch® Unified Endpoint Management and Microsoft® EM+S with Intune. Workspace ONE delivered a better user experience, had more features, and saved time on many device management tasks compared to EM+S. By spending less time on digital workspace and device management tasks, as well as having a better experience, your IT admins can have more time to devote to other key initiatives in your company. In addition, the sooner an admin finishes necessary management tasks, the sooner the device and digital workspace is ready for use.

As you read about our findings, you'll see how Workspace ONE can benefit your company, your IT admins, and your users.

VMware Workspace ONE: A better management experience of digital workspaces and devices

Better usability than Microsoft EM+S

A good platform for managing enterprise devices and digital workspaces should offer simple, streamlined console for admins. Whether it's figuring out a next step in deployment or working through daily tasks, Workspace ONE offered an all-around better experience for our admin than EM+S.



Getting Started

More about Getting Started...

Getting Started provides a step by step solution to help configure the enterprise management tools needed to secure and manage your device fleet.

If you would like to learn more about Getting Started and other resources that help answer questions about AirWatch, please watch the included video before you begin.

Getting Started and myAirWatch

Workspace ONE — 89% Completed

- Frictionless access from any employee or corporate owned device
- Secure connectivity to enterprise productivity apps such as email, calendar, contacts, documents and more
- Instant, Single Sign-On (SSO) access to mobile, cloud and Windows applications
- Powerful data security that protects the enterprise and employees against compromised devices

Mobile Device Management — 62% Completed

- Perform actions on MDM enrolled devices such as lock, notify, or enterprise wipe
- Deploy profiles to configure email, restrictions, settings, and more
- Configure compliance rules to ensure security policies are being met in your device fleet
- View how best to manage your devices from the Dashboard and Hub

Content Management — 30% Completed

Using the AirWatch console

Workspace ONE is an integrated platform for the digital workspace, powered by AirWatch unified endpoint management technology. For the purposes of this report, we refer to the console as AirWatch in the process of setting up Workspace ONE.

Perform tasks from a single console on a modern browser

Using Workspace ONE to manage devices required only the AirWatch console. Admins use this console to do things such as create users, deploy applications, and deploy content after enrollment. Using EM+S to complete the same processes, however, required multiple consoles.

Key usability takeaways from testing and analysis

It wasn’t always clear where admins should perform certain tasks in Intune

After creating our EM+S account, the platform instructed our admin to connect on the old Azure console. A page on that console encouraged us to “Check out the new portal”, which led us to the new Azure console. We used the new Azure console for most of our testing. When we weren’t using that console, it was easier to use the classic Intune console to configure some settings than to do so using the old Azure console.

Certain browsers can make using Intune complicated

The new Intune console in Azure had a link to the classic Intune console. When we opened that link in the modern browsers Google Chrome™ and Microsoft Edge, we received an error. Accessing the classic Intune console required Internet Explorer® due to its Microsoft SilverLight® functionality. Chrome hasn’t supported Silverlight since version 45, Firefox® hasn’t supported it since version 52, Safari® hasn’t supported it since version 5, and Edge has never supported it. What’s more—Internet Explorer did not allow us to save passwords or use the extensions that maintained workflow.

Navigating the AirWatch console was easier

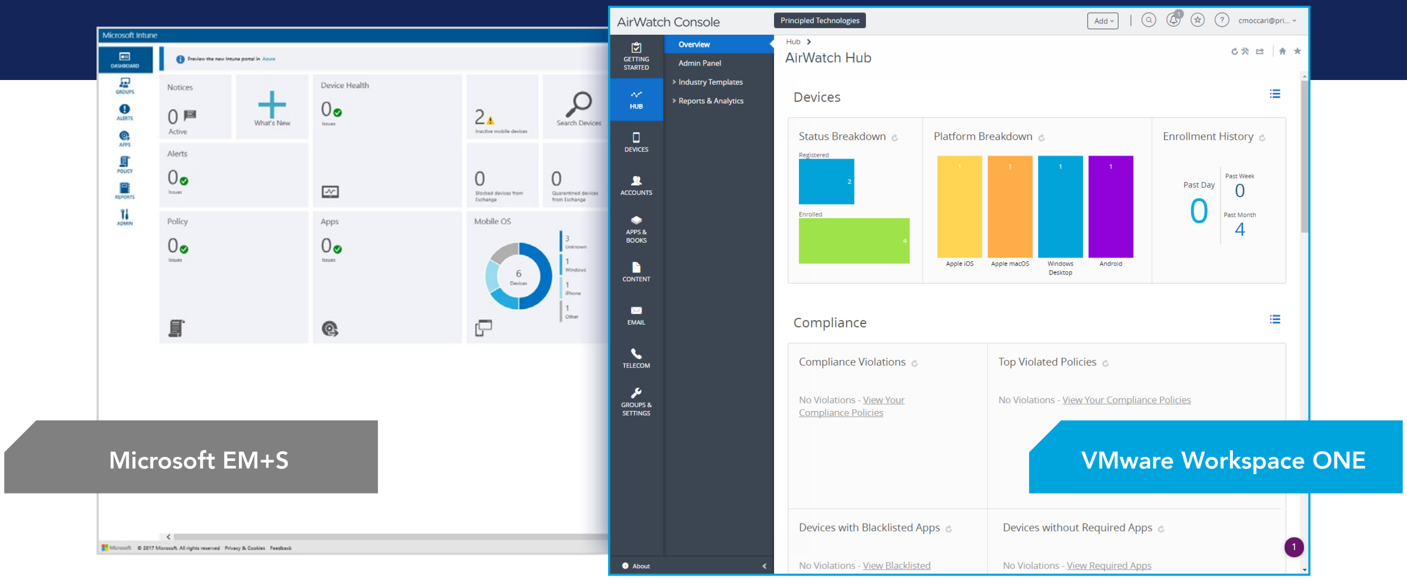
The AirWatch console offered easily discoverable sections such as Getting Started, Hub, Devices, Accounts, Apps & Books, Content, Email, Telecom, and Groups & Settings. The new Azure console offered these tasks as well, but finding and accessing them was not intuitive, and unnecessary add-ons such as VMs, a SQL Server® database, and a Virtual Network cluttered the console’s design. A streamlined, simple console can help save time for your administrator (see the section “Save management time for IT staff and deliver devices to users sooner” for more analysis).

Setting up new technologies was easier

The AirWatch console had a top level to help admins set up new technologies. Getting started with AirWatch was easy as was adding new functionality. After signing up for a trial account, AirWatch lead us though each step of their console.

Guided Tutorials allow admins using AirWatch to track their progress easily, discover new content, and simplify troubleshooting

Tutorials tracked the progress of each task the Administrator performed to set up AirWatch. Administrators could then see the next steps to continue. When we left a tutorial in the middle of playback, the tracker showed the percentage completed. We returned to the tutorial and after clicking Configure, the video resumed playback where we left off.



Our admin felt as if they were on their own when using Intune. When we first started using EM+S, we saw steps to integrate our domain with Intune by installing the enterprise connector. After that, the Intune console offered no next steps. For example, nothing appeared to tell us that we needed to assign an application to user groups after we created the application. If an admin using EM+S and Intune is uncertain why an application isn't deploying or a setting isn't working as expected, they will likely need to delve into the TechNet documentation.

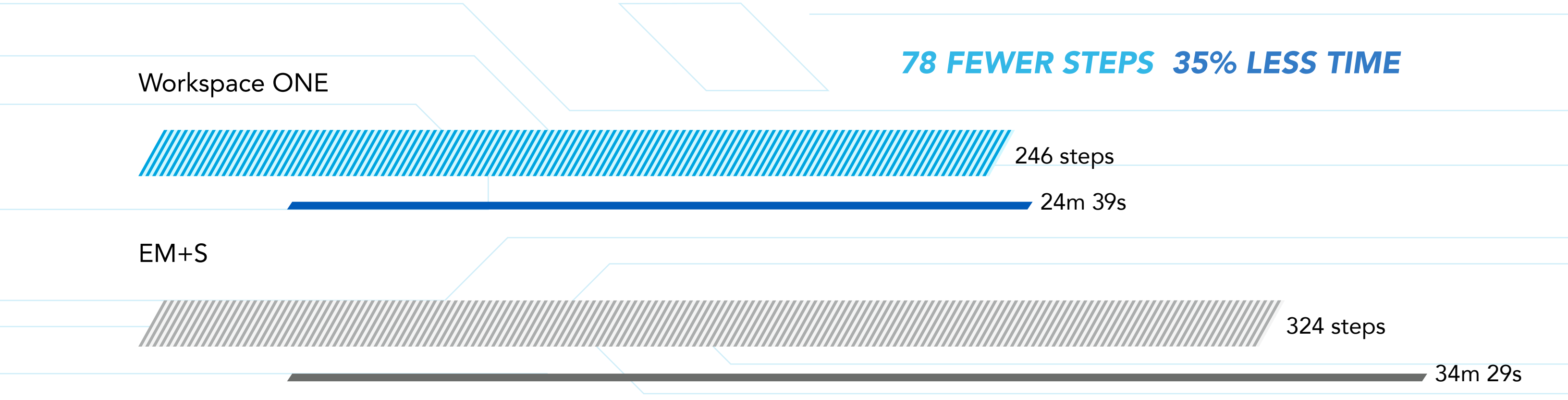
Save management time for IT staff and deliver devices to users sooner

Scenario overview: Setting up a mobility management solution

Admins will likely face a number of common processes when setting up either of the mobility management solutions we tested: setting up an organization, creating a user, enrolling one of each device we tested, and deploying apps and profiles. We measured the time and steps it took each solution to complete the individual tasks of these processes. Compared to using EM+S and Intune, Workspace ONE powered by AirWatch took 78 fewer steps and 35 percent less time to complete all the tasks in the scenario. The tasks and assumptions of our scenario serve as a sample; the size of your user base and the quantity and type of devices your organization uses may alter the time and effort needed from your admins. For a list of tasks in our scenario and detailed results, see Appendix C.

1
Set up an organization
2
Set up users
3
Enroll devices
4
Deploy apps
5
Deploy profiles

Total steps and time to complete all scenario processes



Set up an organization more quickly

Before doing any device or digital workspace management, admins must first get the solution up and running properly. These processes in our scenario included tasks such as logging into the solution for the first time and configuring OS-specific requirements. We started with a Windows Active Directory® server for each solution and built organizations in both. For the "Set up an organization" process in the scenario, it took 7 fewer steps and 47 percent less time to complete the tasks using Workspace ONE. We used the trial versions of the solutions, so times and steps could vary when using the fully licensed versions.

Create a user more quickly

The sooner your admin can create a new user, the sooner they can start preparing the user's device and digital workspace. It took 42 fewer steps and 43 percent less time using Workspace ONE and AirWatch than it did using EM+S and Intune to complete the tasks in the "Set up users" process of the scenario. We assumed the admin in our scenario would create four users separately—one for each device we tested. Both platforms support creating multiple users at once, but based on our assumptions, we timed the task to create one user using each solution and extrapolated the results as four independent tasks.

Enroll a device quickly and with more flexibility

A reality in modern business is that a user's productivity is fairly limited without a device. Saving time getting devices ready to use, particularly mobile devices, puts them in the hands of your users sooner. The solutions had comparable times when completing the tasks in the "Enroll devices" process—our admin needed only a second more when using Workspace ONE.

Devices we used

In addition to studying the capabilities of the overall solutions, we enrolled and deployed profiles and applications to four devices:

Lenovo® Thinkpad® X1 Carbon (4th Generation)
Microsoft Windows 10 Creators Update

Apple® iMac® (Retina 5K, 27-inch, late 2015)
macOS Sierra

Google Nexus™ 6P
Android 7

Apple iPhone® 6S Plus
iOS 10.3

Enrollment emails and a self-service console enable users to perform some management tasks on their own, which can reduce IT time and effort. Upon creating a user, Workspace ONE sent an email to the user with login information and enrollment instructions. Either IT or a user can complete enrollment. This was not always the case with Intune—it did not support automated enrollment emails or a native application for a company console for macOS. Company console applications allow users to self-enroll and download applications to suit their needs.

Deploy apps more quickly and easily

Apps enable users to perform a number of functions with their devices. The faster admins can deploy apps to devices, the sooner users can find answers to questions, draft a note, or schedule an appointment. It took 25 fewer steps and 44 percent less time using Workspace ONE to complete the tasks in the "Deploy apps" process.

In both consoles, admins can visit an app store, select an app, and send it to a group of users. In addition to deploying internal apps more quickly, using Workspace ONE to deploy public apps was faster than using EM+S as well. For example, our admin using Workspace ONE deployed a public Windows 10 app in 29 seconds but it took 58 seconds to deploy the same app using EM+S.

Faster response times using Workspace ONE

Platform response time plays a role in how quickly processes complete. EM+S has more databases that have to communicate, so doing anything in EM+S may take longer. Our admin noticed delays during testing and timed how long it took for a "lock device" command to be issued on the iPhone. The max response time when using Workspace ONE was 1.63 seconds. When using EM+S, the max response time was 33.09 seconds. The less that admins wait on the platform, the sooner they can complete management processes.

What are profiles?

Profiles dictate what options users have on their device. Profiles can define settings for a device, restrict users from completing certain actions, set requirements for password length, or restrict a user from using power controls on their computer. Defining and restricting profiles helps protect your organization from unwanted behaviors.

Deploy profiles more quickly

It took 14 fewer steps and 31 percent less time using Workspace ONE to complete the tasks in "Deploy profiles" than using EM+S. In addition, we created an encryption profile for Bitlocker® (a more complicated task) in less than a minute.

Scenario wrap-up: Workspace ONE reduced effort and saved overall time for an admin

The processes in our scenario represent workflows that an admin will likely have to complete with either mobile management solution. When admins save time and effort completing these routine tasks, they can spend more time on other key initiatives for the organization and put ready-to-use devices into the hands of users sooner, which can help your users be more productive for your organization.

Process	Fewer steps	Less time
Set up an organization	7	47%
Set up users	42	43%
Enroll devices	-10	--
Deploy apps	25	44%
Deploy profiles	14	31%

Manage devices and digital workspaces with better accuracy and flexibility

How organizations enforce compliance with company standards, policies, and workflows can take a number of forms. One effective approach is to control what devices and digital workspaces can do and how users use them. Admins using Workspace ONE can do more when it comes to management than if they use EM+S.

Key manageability takeaways from testing and analysis

Management of Windows 10 devices and digital workspaces is limited when using EM+S

There are two approaches to Windows 10 device and digital workspace management when using EM+S, and you can select only one: choosing to manage the device as a laptop or as a mobile device. As they manage different settings, admins using EM+S must first decide which settings they want to control.

Both approaches have limitations. If an admin chooses to control a device as a computer, the admin cannot use conditional access, device profiles, or agentless enrollment. If an admin chooses to configure the device as a mobile device, the admin cannot deploy .exe or .zip files as applications, configure Windows Firewall settings, or configure Bitlocker encryption.

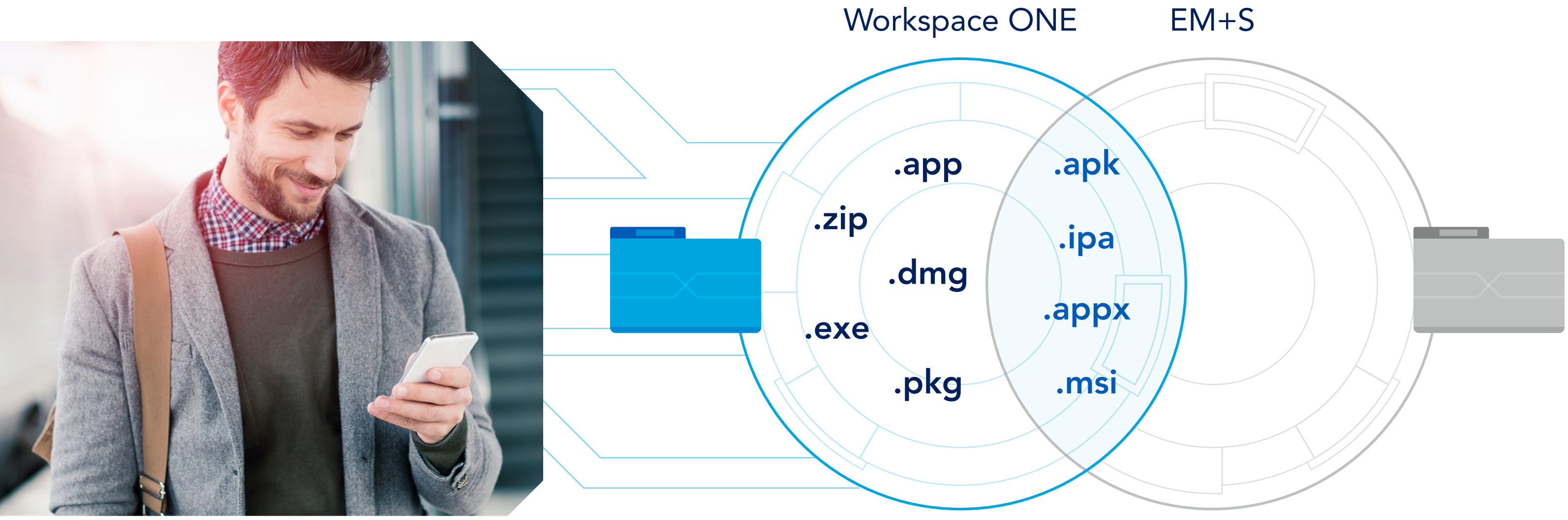
An admin using Workspace ONE for Windows 10 devices and digital workspaces can control all the settings that EM+S can't. Workspace ONE did not make a distinction between managing the device as a computer or as a mobile device.

Workspace ONE had more profile settings on all the devices we tested

Profiles can define what users do on their devices, which helps to keep an organization safe.

Workspace ONE supported more types of apps

We uploaded many file types that EM+S simply didn't support but that Workspace ONE did. We investigated multiple types of app deployment options from each platform. These included public, internal, and volume-purchasable apps. Public apps are available on the device's respective app store. Internal applications are not available on an app store and must be uploaded by the admin to the cloud. These include IPAs for iOS, APKs for Android, DMGs for macOS, and EXEs or ZIPs for Windows. An organization can develop these apps internally or they can download them from a provider.



EM+S could deploy only web apps to the iMac running macOS

The platform didn't support public, internal, or volume-purchasable apps for macOS. Digital workspaces on iMacs managed by the EM+S platform could be very limited in what they could do.

Workspace ONE supported more policies for each device

Admins using Workspace ONE can have a wide selection of policies to apply to user's device regardless of OS. Policies that restrict users, such as disabling iTunes® on iOS or Game Center on macOS, can allow admins to enforce corporate culture while ensuring device security. Policies such as CalDAV and CardDAV configurations for Apple devices can help standardize operational workflows.

Admins using Workspace ONE can troubleshoot connectivity issues

Some features, such as the VMware Connector Tunnel or domain integration, required a connection to an external component. When a feature in the console needed network configuration, a test connection button ran a command. If a failure occurs, the console will indicate the location of the failure.

Secure devices more thoroughly

In today's digitally focused world, securing heavily used devices is essential. Both platforms offered detailed security approaches, but Workspace ONE allowed admins to do more to protect users and organizations.

Key security takeaways from testing and analysis

Bitlocker Encryption is limited for Windows 10 devices and digital workspaces managed by EM+S

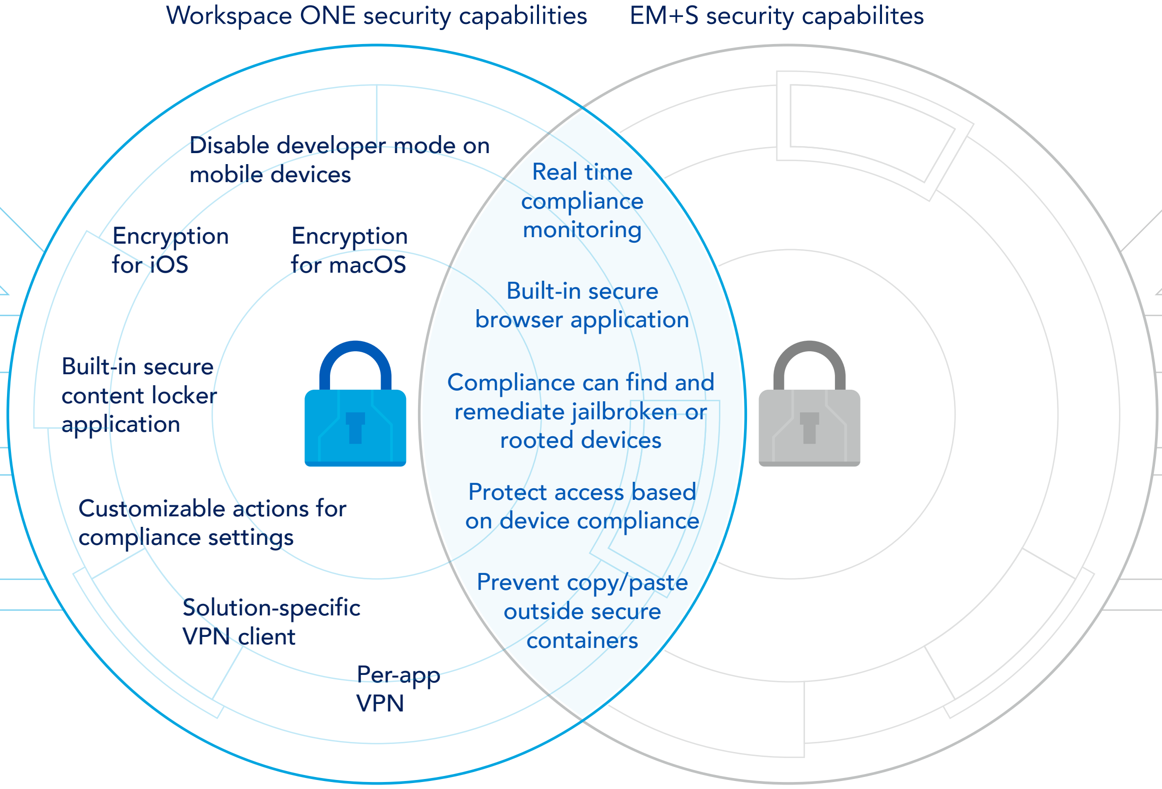
We used Workspace ONE to configure Bitlocker Encryption and deploy it to the Windows 10 digital workspace in our organization. The process took less than 31 seconds. Within a few seconds after completing the configuration, a notification showed up on our ThinkPad laptop confirming that Bitlocker encryption was underway. EM+S could not configure Bitlocker Encryption when managing Windows 10 devices as mobile devices. Workspace ONE even configured TPM and BIOS passwords to meet encryption requirements.

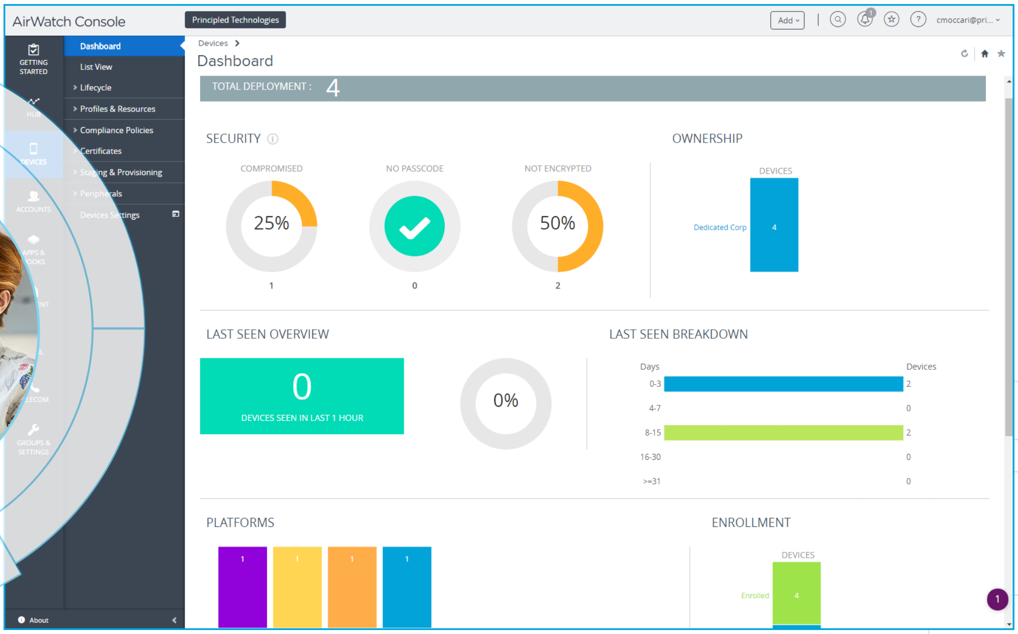
Workspace ONE had more remediation options for device and digital workspace compliance issues

Compliance settings for either platform can discover if an OS is out-of-date, jailbroken, rooted, or simply not password-policy compliant, but admins using Workspace ONE can decide best how to solve the issue by choosing from more remediation options. For example, an administrator could deploy a policy and fix an issue, or they could set up a message template that encourages users to fix the issue themselves and set up a follow-up message template. These options give admins and organizations flexibility in their approach to remediation.

Workspace ONE had more security policy options

The options that only Workspace ONE offered could improve safety for the organization. For example, an admin using Workspace ONE or EM+S could set requirements for device passwords and biometric sign in on any of the devices we tested. Only an admin using Workspace ONE for Android devices, however, could disable developer options, set anti-virus settings, or disable video recording. Using Workspace ONE, an admin could also restrict Apple users from syncing their key chain to iCloud. This restriction prevents user passwords for an organization's apps from being transferred to another organization.


Workspace ONE security capabilities
EM+S security capabilites
Disable developer mode on mobile devices
Encryption for iOS
Encryption for macOS
Built-in secure content locker application
Customizable actions for compliance settings
Solution-specific VPN client
Per-app VPN
Real time compliance monitoring
Built-in secure browser application
Compliance can find and remediate jailbroken or rooted devices
Protect access based on device compliance
Prevent copy/paste outside secure containers



Conclusion

Overall, we found Workspace ONE provided administrators with the tools and information they needed to quickly and effectively manage an organization. If admins in your organization could benefit from a feature-rich enterprise platform that manages devices and digital workspaces better, deploys apps more quickly, supports Windows 10 devices fully, and supports better security, consider Workspace ONE powered by AirWatch Unified Endpoint Management.

On July 10, 2017, we finalized the hardware and software configurations we tested. Updates for current and recently released hardware and software appear often, so unavoidably these configurations may not represent the latest versions available when this report appears. For older systems, we chose configurations representative of typical purchases of those systems. We concluded hands-on testing on August 4, 2017.

Appendix A: System configuration information

Device configuration information	Apple iPhone 6s Plus	Google Nexus 6P
Processor		
Vendor	Apple	Qualcomm
Name	Twister	Snapdragon
Model number	A9 + M9 coprocessor	810
Core frequency	1.85 GHz	1.95 GHz + 1.55 GHz
Number of cores	2	8 (4 + 4)
Memory		
Amount	2 GB (built-in onboard)	3 GB (built-in onboard)
Type	LPDDR4	LPDDR4
Graphics		
Vendor	Imagination Technologies	Qualcomm
Model number	PowerVR GT7600	Adreno 430
Storage		
Amount	64 GB	64 GB
Type	NAND Flash	NAND flash
Connectivity		
Wireless internet	802.11ac (802.11a/b/g/n compatible)	802.11ac (802.11a/b/g/n compatible)
Cellular	LTE Advanced	LTE Advanced
Bluetooth	4.2	4.2
Battery		
Type	Lithium-polymer	Lithium-polymer
Size	Integrated	Integrated
Rated capacity	10.45 Wh	13.11 Wh
Display		
Size	5.5”	5.7”
Type	LED-backlit widescreen Multi-Touch	AMOLED widescreen Multi-Touch
Resolution	1,080 x 1,920	1,440 x 2,560

Device configuration information	Apple iPhone 6s Plus	Google Nexus 6P
Cameras		
Front-facing	5MP 720p FaceTime® HD	8 MP
Rear-facing	12MP iSight®	12.3 MP
Operating system		
Vendor	Apple	Google
Name	iOS	Android
Build number or version	10.3.3	7.1.2
Dimensions		
Height	6.23"	6.27"
Width	3.07"	3.06"
Depth	0.29"	0.28"
Weight	6.77 ounces	6.27 ounces

Device configuration information	Lenovo ThinkPad X1 Carbon (4th Generation)	Apple iMac (Retina 5K, 27-inch, Late 2015)
Processor		
Vendor	Intel®	Intel
Name	Core™ i7	Core i7
Model number	2.60	4
Core frequency	2	4
Number of cores	4 MB L3	8 MB L3
Memory		
Amount	8	32
Type	DDR3	DDR3
Graphics		
Vendor	Intel	AMD
Model number	HD Graphics 520	Radeon R9 M390
VRAM	4 GB	2 GB
Storage		
Amount	256 GB SSD	24 GB SSD with 1TB HDD
Connectivity		
Wired internet	Intel Ethernet Connection I219-LM	Broadcom Gigabit Ethernet
Wireless internet	Intel Dual Band Wireless-AC 8260	Airport Extreme 802.11ac Wi-Fi
Bluetooth	4.0	4.0

Device configuration information	Lenovo ThinkPad X1 Carbon (4th Generation)	Apple iMac (Retina 5K, 27-inch, Late 2015)
USB	3 x USB 3.0	4 x USB 3.0
Thunderbolt™	1	2
Video	1 x HDMI	1 x Mini DisplayPort
Display		
Size (in.)	14”	27
Type	HD LED WXGA	Retina 5K display with IPS technology
Resolution	1,920 x 1,080	5,120 x 2,880
Touchscreen	No	No
Operating system		
Vendor	Windows	Apple
Name	Windows 10	macOS Sierra
Build number or version	10.0.15063	10.12.6

Appendix B: How we tested

Completing the common setup

Our test used a preconfigured Windows Server® 2016 Datacenter Edition Hypervisor. We created two virtual machines with 4 virtual processors and 8 GB of memory and connected our Windows Server 2016 media to the system.

Installing Windows Server 2016 Datacenter Edition

1. Right click the target VM, and select Connect.
2. Click the power on button.
3. When requested, press any key to boot to the virtual media.
4. On the Windows Server 2016 screen, click Next.
5. Click Install Now.
6. On the Activate Windows Screen, click I don't have a product key.
7. Select Windows Server 2016 Datacenter (Desktop Experience), and click Next.
8. Agree to the License.
9. Select Custom Installation.
10. Select the target volume for the Windows installation, then click Next.
11. Wait for the installation to complete.
12. At the Customize settings screen, enter, confirm a password, and click Finish.

Configuring Windows Server 2016

1. At the login screen, enter your password, and press enter.
2. Open Windows Update, and press Check for updates.
3. Allow the updates to install.
4. Open Windows Firewall with Advanced Security.
5. Click Windows Firewall Properties.
6. On the Domain Profile, Private Profile, and Public Profile tabs, set the Firewall state to off.
7. Open System Properties.
8. In the Remote tab, select Allow remote connections to this computer. Click to deselect the Allow Connections only…. checkbox. Click OK.

Measuring time and steps

Throughout the following methodology, we start our time right before the first step and stop it as we complete the final step. You can find times for each of the tasks in Appendix 3.

When we refer to the Intune console, we mean the console at https://manage.microsoft.com. When we refer to the Azure console, we mean the portal at https://portal.azure.com.

Setting up an organization

Workspace ONE

Requesting the trial

1. Navigate to https://www.air-watch.com/lp/free-trial/.
2. Fill in the contact information, and click Start your Free Trial.

Completing the initial login

1. Check your email, and open the Welcome to AirWatch email.
2. Click the Console URL link.
3. Enter the included AirWatch information, and click Login.
4. On the Terms of Use screen, click Accept.
5. You will be redirected to the Security Settings screen. For Password Recovery Question 1, enter a Password Recovery Answer and confirm the Password Recovery Answer.
6. For Security PIN, enter a 4 digit Security PIN, and confirm the Security PIN.
7. On the AirWatch 9 Console Highlights screen, click "Don't show this message on login", and click the X to close the window.

Installing software for the Enterprise Connector

1. On the target active directory server, in Server Manager, click Add roles and features.
2. On the Add Roles and Features Wizard, select Skip this page by default, and click Next.
3. On the Installation Type screen, click Next.
4. On the Server Selection screen, click Next.
5. On the Server roles screen, select Web Server (IIS). For the popup, click Add Features. Click Next.
6. On the Features screen, click Next.
7. On the Web Server Role screen, click Next.
8. On the Role Services screen, click Next.
9. On the confirmation screen, click Install.

Installing the Enterprise Connector

1. From the target Active Directory server, in the AirWatch Console, click the Groups & Settings workspace.
2. Select All Settings.
3. In the Settings window, on the System panel, under Enterprise Integration, select VMware Enterprise Systems Connector.
4. Change the Current Setting to Override. Select Enable VMware Enterprise Systems Connector. Click Save.
5. Navigate to Enterprise Integration > Enterprise Integration Services, and change the current setting to Override. Click Save. Close the Settings panel.
6. Click the Getting Started Workspace.
7. Next to Workspace ONE, click Continue.
8. Next to Enterprise Connector & Directory, click Configure.
9. On the VMware Enterprise Systems Connector Setup screen, enter and confirm a password, then click to download the VMware Enterprise Systems Connector Installer.
10. Run the VMware Enterprise Systems Connector Installer.
11. When prompted, on the VMware Enterprise Systems Connector –InstallShield Wizard, install the Microsoft .NET Framework 4.6.2 by clicking Install.
12. In the AirWatch Enterprise Integration Wizard, wait for the wizard to finish preparing the program, and click Next.
13. On the License Agreement screen, click I accept the terms in the license agreement.
14. On the Custom Setup screen, click Next.
15. On the Destination Folder screen, click Next.
16. On the ACC Certificate Password screen, type your previously entered Certificate Password, and click Next.
17. On the Proxy Information screen, click Next.
18. On the Ready to Install the Program screen, click Install.
19. Once the Installation is complete, click Finish.
20. Return to the AirWatch console. On the Active Directory screen, keep the automatically populated information, and fill in your login information and the FQDN of your server. Click Save. Click Test Connection.

Completing the additional configuration

1. In the AirWatch Con to Groups & Settings, under Devices & Users > General, click Notifications.
2. On the Notifications Screen, select Override.
3. For Devices Unrolled, select Send email to User.
4. For Device Enrolled Successfully, select Send email to User.
5. For Devices Blocked by Enrollment Restriction, select Send email to User. Click Save.

Configuring Apple Push Notification Service for Apple Enrollment

1. In the AirWatch Console, select the Getting Started workspace, and select Workspace One.
2. Next to Apple Push Notification Service (APNs), click Configure.
3. On the APNs screen, select the MDM_APNsRequest.plist download to download the file.
4. When requested by your system, click Save.
5. Click Continue.
6. For Create an Apple Certificate, select Don't have a Corporate Apple ID.
7. On the Corporate Apple ID popup, click Create Account with Apple.
8. After you're redirected to AppleID.apple.com, click Create Your Apple ID.
9. On the Create Your Apple ID page, fill in the appropriate information. When finished, click Submit.
10. Verify your account by retrieving the verification code.
11. Enter the code, and click Continue.
12. Return to the AirWatch console, and close the popup.
13. Enter your Corporate Apple ID.

14. Click the link for Apple Push Certificates Portal.
15. Sign in using the credentials for the account you created in Step 9.
16. On the Apple Push Certificates Portal webpage, click Create a Certificate.
17. Check I have read and agree to these terms and conditions, and click Accept.
18. On the Create a New Push Certificate screen, click Choose File, and select the MDM_APNsRequest.plist file that you downloaded before. Then click Upload.
19. On the Confirmation screen, click Download.
20. Return to the AirWatch console, and click Continue.
21. On the Upload Apple Certificate screen, click Upload.
22. On the Add Window, click Choose File, and select the MDM_ AirWatch_Certificate.pem file you downloaded before.
23. Click Save.
24. Click Finish. You now automatically browse to the AirWatch Express Console.

Setting up Android for Work

1. In the AirWatch Console, click the Groups & Settings workspace.
2. Click All Settings.
3. In the Settings Window, in the panel, under Devices & Users, Android, click Android for Work.
4. On the Android for Work screen, click Configure.
5. On the Bring Android to work screen, sign in with your Gmail admin account.
6. Click Get Started.
7. On the Organization details screen, enter your Organization name.
8. Check the box for I have read and agree to the Managed Google Play Agreement, and click Continue.
9. On the Set up complete screen, click Complete Registration.
10. Under Auto-Enrollment, click Override, then Enable Auto-Enrollment. Click Save.
11. Under Service Applications, click Override, then Enable Push Service App from Play Store. Click Save.

EM+S

Requesting the trial

1. Navigate to https://signup.microsoft.com/Signup?OfferId=87dd2714-d452-48a0-a809-d2f58c4f68b7&ali=1.
2. Enter your information, and click Next.
3. On the User ID information, enter your information, and click Create my account.
4. On the Prove. You're. Not. A. Robot. screen, select Text me, and enter a phone number for verification. Then click Text me.
5. On the Verification screen, enter the verification code delivered to your phone number, and click Next.
6. On the Save this info screen, click You're ready to go…

Completing the initial login

1. After completing registration, your browser will redirect to the Get Started page. For Step 1, click Start.
2. Click the link to sign up for an Azure trial subscription.
3. On the About you tab, enter your information. It may autofill based on the information provided in the previous section. Click Next.
4. On the Identify verification by phone tab, click Send text message.
5. After receiving the text message, enter the verification code, and click verify code.
6. On the Identify verification by card tab, enter your credit card information and click Next.
7. On the Agreement tab, click the checkbox next to I agree, and click Sign up.
8. Once your subscription is completed, click Get started with your Azure subscription.

Configuring and installing the software for the Enterprise Connector

1. On the target VM, in Server Manager, click Add roles and features.
2. On the Add Roles and Features Wizard, select Skip this page by default, and click Next.
3. On the Installation Type screen, click Next.
4. On the Server Selection screen, click Next.
5. On the Server roles screen, select Active Directory Certificate Services and Remote Access. For the popup, click Add Features. Click Next.
6. On the Features screen, click Next.
7. On the Remote Access screen, click Next.
8. On the Role Services screen, select Web Application Proxy, and click Next.
9. On the Confirmation screen, click Install.

10. In Server Manager, click the flag, and select Configure the Certificate Authority.
11. In the AD CS Configuration window, click Next.
12. On the Role Services screen, select Certification Authority, and click Next.
13. On the Setup Type screen, select Enterprise CA, and click Next.
14. On the CA Type screen, select Root CA, and click Next.
15. On the Private Key screen, click Next.
16. On the Cryptography screen, click Next.
17. On the CA Name screen, click Next.
18. On the Validity Period screen, click Next.
19. On the Certificate Database screen, click Next.
20. On the Confirmation screen, click Install.

Install the Enterprise Connector

1. During EM+S setup, return to the Enterprise Mobility + Security tab in your browser.
2. Click Step 2.
3. Under Step 2, click Start.
4. In the Microsoft Azure Portal, under Active Directory, Directory, click the name of your organization.
5. On the Active Directory starting page, under Get Started, click Add domain.
6. On the Specify a domain name, type a domain name, and click add. We used `printechlabs.local`.
7. Click Next.
8. On the Verify domain screen, note the information for the text record.
9. Add the text record to your domain in your registrar. It can take up to 24 hours for these changes to propagate.
10. In the Azure portal, click verify.
11. In the Azure Portal, click the link to download the Azure AD Connector.
12. Once the download is complete, double click the executable to start the installer.
13. In the Microsoft Azure Active Directory Connect Wizard, click Continue.
14. On the Express Settings screen, click Use Express Settings.
15. On the Connect to Azure AD screen, enter your Azure AD credentials. These are used to log into Microsoft online.
16. On the Connect to AD DS, enter your user name and Password for your local active directory.
17. On the Azure AD sign-in screen, click Next.
18. On the Ready to configure screen, click Install.

Configuring Apple Push Notification Service for Apple Enrollment

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune panel, click Device enrollment.
3. On the Device enrollment panel, click Apple enrollment
4. On the Apple enrollment screen, click Enrollment Program Token.
5. On the Enrollment Program panel, click to set up.
6. Under Steps to configure an enrollment program token, click Download your public key.
7. Click Create a token via Apple Device Enrollment Program.
8. On the Apple Deployment Programs page, click Don’t have an account Enroll now.
9. On the Welcome screen, Next to Click Device Enrollment Program.
10. On the Add Verification Contact Details screen, click Next.
11. On the Add Institution Details screen, enter all necessary information, and click Next.
12. On the Review Your Enrollment Details screen, click Submit.
13. Once the review is complete, you will receive a call from an Apple employee verifying accounts settings.
14. Log ino deploy.apple.com.
15. On the Terms and Conditions screen, check the box indicating “I have read and agree to the APEP Agreement”. Then click Agree.
16. On the Terms and Conditions screen, agree to the macOS Software License Agreement, and click Agree.
17. Agree to the iOS Software License Agreement, and click Agree.
18. In the Apple Deployment Program console, select Manage Servers.
19. On the Manage Servers screen, click Add.
20. On the Add MDM Server screen, give your MDM Server a name, check the box for Automatically Assign New Devices, and click Next.
21. On the Upload your Public Key screen, click Choose File, and select your Public Key from Step 2. Then click Next.
22. Click the link to Download your Server Token. Click Done.
23. In the Intune Dashboard, enter the Apple ID used to create your token.
24. Click the folder icon in step 4, and select the Server Token downloaded in step 18. Click Upload.

Setting up Android for Work

1. In the Intune console, select the Admin Workspace.
2. In the Administration panel, select Mobile Device Management.
3. Click Configure Android for Work.
4. On the Android for Work Mobile Device Management Setup, click Configure.
5. On the Google Play Bring Android to work screen, click Sign In.
6. Sign in with a Google account.
7. On the Organization details screen, type your Organization name, check the box to agree to the Google Play agreement, and click Confirm.
8. Click Complete Registration.
9. In the Intune console, select Manage supported devices as Android for Work, and click Save.

Setting up users

Workspace ONE

Adding a new user

Note: We completed this task once and extrapolated the results to reflect four users created separately.

1. In the AirWatch Console, in the Accounts workspace, under users, click List View.
2. Click Add, then Add user.
3. Enter a username, password, full name, and email.
4. Click Save.

Importing multiple new users

Note: We did not include timing for this item in our comparison.

1. In the AirWatch Console, in the Accounts workspace, under users, click List View.
2. Click Add, then Batch Import.
3. In the gray pane, under User And/Or Device, click Download simple template and example for this batch type.
4. Open the Downloaded file.
5. Make any necessary changes, and save as a .csv file. We did not record time for this step.
6. In the portal, enter a Batch Name, Batch Description, and Batch Type. For Batch type, use Users And/Or Devices.
7. Click Import.

Creating a new smart group

1. In the AirWatch Console, select the Groups & Settings workspace.
2. In the Groups & Settings workspace, select Groups, Organization Groups, and Assignment Groups.
3. On the Assignment Groups screen, click Add Smart Group.
4. On the Create New Smart Group screen, enter WinTest for name. Under Platform and Operating System, select "Windows Desktop", "Equals", and "Any". Click Save.

We repeated this step for AndroidTest, macOSTest, and iOSTest.

EM+S

Creating a user

Note: We completed this task once and extrapolated the results to reflect four users created separately.

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune workspace, click the Users and Groups workspace.
3. On the Users and groups panel, click All Users.
4. On the toolbar, click New User.
5. On the User panel, give the user a name and a user name.
6. Click Show Password. Copy the password and record it.
7. Click create.
8. In the User workspace, click the new user.
9. Under Profile, set the Usage Location to United States. Click Save.
10. Click Licenses.

11. On the toolbar, click Assign.
12. Click Products, then select Enterprise Mobility + Security.
13. Click Select.
14. Click Assign.

Creating a new smart group

1. On the Azure Portal, select the Users and groups workspace.
2. Select All Groups.
3. In the All Groups panel, click New Group.
4. In the Group panel, for name, type WindowsTest. For membership type, select Dynamic device. Click Add dynamic query.
5. For Dynamic membership rules, create a rule to Add devices where device OSType, Starts With, Windows. Click Add Query.
6. In the Group panel, click Create.

We created additional smart groups for AndroidTest, macOSTest, and iOSTest.

Enrolling devices

Workspace ONE

Enrolling an iOS Device

1. On the target device, open the AirWatch User Activation email.
2. Tap the link to Set your AirWatch password.
3. On the AirWatch SSP page, enter and confirm your new Password, and tap Submit.
4. Return to the email, and click the link to awagent.com to download the AirWatch Agent app.
5. On the Download page, click Go to Apple AppStore.
6. In the Apple AppStore AirWatch Agent page, tap Get, then Install. Once the installation completes, open the application.
7. On the Authenticate screen, select email.
8. On the Authenticate screen, enter the domain email address, and click Continue.
9. On the User Credential page, enter your username and password, and tap Next.
10. On the Enable Device Management screen, tap Redirect and Enable.
11. On the Install Profile screen, tap Install.
12. Enter your PIN.
13. Tap Install.
14. On the Warning screen, tap Install.
15. On the Remote Management popup, tap Trust.
16. On the App Installation popup, tap Install.

Enrolling an Android device

1. On the target Android device, open the AirWatch User Activation Email.
2. In the AirWatch User Activation email, tap the link to set your AirWatch Password.
3. On the AirWatch SSP screen, enter and confirm your new password.
4. In the activation email, tap the link to download the AirWatch Agent app.
5. In the Google Play Store, click Install.
6. Once the download is complete, tap open.
7. On the Welcome to AirWatch! Screen, tap email address.
8. On the Authenticate screen, enter the domain email address, and click Continue.
9. On the Welcome to AirWatch! Screen, click Continue.
10. At the Authenticate screen, enter your user credentials, and tap Continue.
11. At the Set up work profile screen, tap Next.
12. On the admin popup, tap OK.
13. On the Create your Work App password screen, tap Device Settings.
14. On the Unlock section screen, select Continue without Nexus Imprint.
15. On the Unlock selection screen, select PIN.
16. Enter and confirm your PIN, and click OK.
17. On the Notifications screen, click Done.
18. On the Confirm your PIN screen, enter your work PIN, and hit enter.

Enrolling a macOS device

1. On the target device, open the AirWatch User Activation email.
2. In the Activation Email, click the link to Set your AirWatch password.
3. On the AirWatch SSP page, enter and confirm your new password, and click Submit.
4. Return to your email, and open the AirWatch Device Activation email.
5. In the Activation email, click the link for awagent.com.
6. On the Download page, click Download.
7. Once the download completes, click AirWatchAgent.dmg to run the installer.
8. Click VMware AirWatch Agent.pkg.
9. On the Welcome to the VMware AirWatch Agent Installer, click Continue.
10. On the License screen, click Continue.
11. On the popup, click Agree.
12. On the Installation Type screen, click Install. If prompted, enter your password.
13. Once complete, click close.
14. Open the VMware AirWatch Agent.
15. On the Status screen, click Enroll Now.
16. On the Authentication screen, click Authenticate Email.
17. On the Email screen, enter your email.
18. On the Welcome to AirWatch! Screen, click continue.
19. On the Enter your credentials screen, enter your credentials, and click Continue.
20. On the Enable Device Management screen, click Enable.
21. Enter your computer password when prompted.

Enrolling a Windows 10 device

1. On the target device, open the AirWatch User Activation email.
2. In the Activation email, click the link to Set your AirWatch password.
3. On the AirWatch SSP page, enter and confirm your new password, and tap Submit.
4. In the Activation email, click the link for awagent.com.
5. On the Download page, click Download.
6. Click Run.
7. In the AirWatch Agent installation wizard, when asked to install Microsoft Visual C++2013, click OK.
8. On the Welcome screen, click Next.
9. On the License Agreement screen, accept the license agreement, and click Next.
10. On the Read to Install the Program screen, click Install.
11. Once complete, click Finish.
12. On the User Account Control screen, to allow Native Enrollment to make changes to your device, click Yes.
13. When VMware AirWatch Agent authentication screen appears, select email activation.
14. On the Authenticate screen, enter the domain email address, and click Continue.
15. On the Welcome to AirWatch! screen, click Next.
16. On the Enter Credentials screen, enter your user name and password, and click Next.
17. Once complete, click Finish.

EM+S

Enrolling an iOS device

1. On the iPhone, open the App Store.
2. Search Intune Company Portal.
3. Tap Get then Install Microsoft Intune Company Portal. If requested, enter your password.
4. Once the installation is complete, launch the Microsoft Intune Company Portal app.
5. Sign in using your user credentials.
6. At the Update your Password screen, enter and confirm a new password. Tap Update password and sign in.
7. On the Company Access Setup screen, tap Begin.
8. On the Why enroll your device? Screen, tap Continue.
9. On the We care about your privacy screen., tap Continue.
10. On the What comes next screen?, tap Enroll.
11. When the setting app opens, tap Install, and enter your PIN if requested.

12. Tap Install on the popup.
13. On the Warning screen, tap Install.
14. On the Remote Management popup, tap Trust.
15. After installation finishes, tap done.
16. In the Safari web browser, tap Open.
17. On the Company Access Setup screen, you should see green checkmarks for Device Enrollment and Device Compliance. Tap Continue.
18. On the Company Access Setup Complete screen, tap Done.

Enrolling an Android device

1. On the Android device, open the Google Play store.
2. Search for the Intune Company Portal App.
3. Tap Install.
4. Once complete, open the Intune Company Portal App.
5. Login with your user credentials.
6. At the Update your Password screen, enter and confirm a new password. Tap Update password and sign in.
7. On the Terms screen, tap Accept.
8. On the Company Access Setup screen, tap Begin.
9. On the Why create a work profile? screen, tap Continue.
10. On the We care about your privacy. screen, tap Continue.
11. On the What comes next? screen, tap Continue.
12. On the Set up work profile screen, tap Next.
13. Tap OK.
14. Once loaded, click Sign in.
15. Sign in using your credentials.
16. On the Company Access Setup screen, tap Continue.
17. Once your device has been enrolled, tap Register your Device.
18. Tap Continue.
19. On the Company Access Setup complete screen, tap Done.

Enroll a macOS device

1. Open Safari and navigate to portal.manage.microsoft.com.
2. On the Microsoft Intune login page, log in with your user credentials.
3. On the Update your password screen, enter the current password. Then enter and confirm a new password. Click Sign in.
4. In the portal, click the hamburger button, and select My Devices.
5. On the My Devices screen, click the notification link to enroll your device.
6. On the Which device is this? screen, click Enroll.
7. On the Enroll this Device screen, click Install.
8. On the Install "Management Profile"? popup, click Install. If prompted, enter your password.
9. Click Continue.
10. Click Install.

Enrolling a Windows 10 device

1. Open the Windows store.
2. Search for the Company Portal.
3. On the Company Portal screen, click Download.
4. Once complete, click Launch.
5. On the Let's get you signed in screen, type your user account.
6. On the Enter password screen, enter your account password, and click Sign in.
7. On the Update your password screen, enter the current password. Then enter and confirm a new password. Click Sign in.
8. On the Add this account to Windows screen, click Yes.
9. On the You're all set! screen, click Done.
10. In the Company Portal screen, under My Devices, click the message to begin setup for corporate Use.
11. On the Set up your device screen, click Next.
12. On the Enroll into management screen, click Enroll this device.
13. On the Set up a work or school account screen, enter the user email address.
14. Enter your user credentials.

15. On the Enroll into management screen, click Next.
16. On the You're all set! screen, click Done.

Deploying applications

Workspace ONE

Deploying an internal application

For timing purposes, we used the "VLC Player 2.2.2.msi" 49.6 MB file to deploy to Windows systems.

1. In the AirWatch Console, select the Devices workspace.
2. On the list view page, on the Internal tab, click Add Application.
3. Select Upload.
4. On the Add screen, click Choose File.
5. Select the target file, and click OK.
6. Click Continue.
7. On the Application screen, click Save & Assign.
8. On the Assignment screen, click the field for Select Assignment Groups, and select WindowsTest. Click Save & Publish.
9. On the View Device Assignment screen, click Publish.

Deploying an internal Apple macOS application

1. In the AirWatch Console, select the Devices workspace.
2. Under Staging & Provisioning, under Components, select Files/Actions.
3. On the Files/Actions screen, click Add Files/Actions.
4. On the Add Files/Actions screen, click Apple macOS.
5. On the General tab, for name enter `Slack`. Click the Files tab.
6. On the Files tab, click Add Files.
7. On the Add Files window, click Choose Files.
8. In the File Explorer, select the "Slack-2.6.3-macOS.zip" 69 MB file, and click Open.
9. Click Save.
10. Once complete, on the Add Files screen, enter the download path `/Users/principledtech/apps/Slack-2.6.3-macOS.zip`. Click Save.
11. Click the Manifest tab.
12. On the Manifest tab, under Install Manifest, click Add Action.
13. On the Add Manifest screen, enter the following:
    a. Action(s) to Perform: Install
    b. File Path and Name to Install: `/Users/principledtech/apps/Slack-2.6.3-macOS.zip`
14. Click Save.
15. Click Save.
16. Under Staging and Provisioning, click Product List View.
17. On the Product List View screen, click Add Product.
18. On the Add Product screen, click Apple macOS.
19. On the Add Product screen, on the General tab, enter the following:
    a. Name: `Slack`
    b. Assigned Groups: `All Devices`
20. Click Manifest.
21. On the Manifest tab, click Add.
22. On the Add Manifest screen, enter the following:
    a. Action(s) to Perform: Install Files / Actions
    b. Files/Actions: Slack
23. Click Save.
24. Click Activate.
25. On the View Device Assignment screen, click Activate.

Deploying a public Android application

1. In the AirWatch console, select the Apps & Books workspace.
2. On the List View screen, click the Public Tab.
3. On the Public tab, click Add Application.

4. On the Add Application screen, for Platform, select Android. Select Search App Store. Under Name, type Slack, and click Next.
5. On the Google Play screen, select Slack.
6. On the Slack screen, click Approve.
7. Click Approve.
8. On the Approval Settings, click Save.
9. On the Assignment screen, click the field for Select Assignment Groups, and select AndroidTest. Click Save & Publish.
10. On the View Device Assignment screen, click Publish.

Deploying a public Apple iOS application

1. In the AirWatch console, select the Apps & Books workspace.
2. On the list view page, on the Public tab, click Add Application.
3. On the Add Application screen, for Platform, select Apple iOS. Select Search App Store. Under Name, type Slack, and press enter.
4. On the Search screen, click Select next to Slack – Business Communication for Teams.
5. On the Add Application screen, click the assignment tab.
6. Click the field for Select Assignment Groups, and select iOSTest. Click Save & Publish.
7. On the View Device Assignment screen, click Publish.

Deploying a public Windows application

1. In the AirWatch console, select the Apps & Books workspace.
2. On the list view page, on the Public tab, click Add Application.
3. On the Add Application screen, for Platform, select Windows Desktop. Select Search App Store. Under Name, type Slack, and press enter.
4. On the Search screen, click Select next to Slack – Business Communication for Teams.
5. On the Add Application screen, click the assignment tab.
6. Click the field for Select Assignment Groups, and select WinTest. Click Save & Publish.
7. On the View Device Assignment screen, click Publish.

Deploying a web app

1. In the AirWatch console, select the Apps & Books workspace.
2. In the Applications workspace, click the Web tab.
3. On the Web tab, click Add Application.
4. On the Add Application screen, for platform, select macOS. Click Continue.
5. On the New Application screen, on the Details tab, type Slack. For URL type, enter https://itunes.apple.com/us/app/slack/id803453959?mt=12. Click the Assignment tab.
6. On the Add Application screen, on the assignment tab, click the field for Select Assignment Groups, and select macOSTest.
7. Click Save & Publish.
8. On the View Device Assignment screen, click Publish.

EM+S

Deploying an internal application

For timing purposes, we used the "VLC Player 2.2.2.msi" 49.6 MB file to deploy to Windows systems.

1. On the Azure Portal, select the Intune Workspace.
2. Select Mobile apps, then apps.
3. Click Add.
4. On the Add app panel, select Line-of-business App.
5. Select App package file, click the blue folder icon to add the app.
6. In the File Explorer, select the VLC Player 2.2.2.msi file, and click OK..
7. Click OK.
8. Under App information, enter a description and publisher. Then click OK.
9. Click Add.
10. You will not be able to assign the file until the VLC player finishes uploading. Once complete, select the VLC Player 2.2.2 app from the app list.
11. In the VLC Player 2.2.2 panel, select assignments.
12. In the Assignments panel, click Select Groups.
13. In the Select groups panel, use the search bar to find and select the WindowsTest group. Click Select.
14. In the Assignments panel, for VLCtest group, select Available for type, and click save.

Deploying an internal Apple macOS application

Intune is not able to deploy internal macOS applications.

Deploying a public Android for Work application

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune Workspace, select Mobile apps.
3. On the Mobile Apps panel, select Android for Work.
4. Click Open the Play for Work Store.
5. In the app store, search for Slack.
6. Select Slack.
7. On the Slack page, click Approve.
8. On the App access page, click Approve.
9. On the Approval Settings screen, click Save.
10. Return to the Azure Portal, and click Sync.
11. In the Mobile apps panel, click Apps.
12. Select Slack.
13. In the Slack panel, click Assignments.
14. In the Assignments panel, click Select Groups.
15. In the Select groups panel, use the search bar to find and select the AndroidTest group. Click Select.
16. For AndroidTest group, select Available for type and click save.

Deploying a public Apple iOS application

1. On the Azure Portal, select the Intune Workspace.
2. Select Mobile apps, then Apps.
3. Click Add.
4. In the Add app panel, for app type, click iOS store app. Click Search the App Store.
5. In the search bar, enter Slack.
6. Select Slack – Business Communication for Teams. Click OK.
7. Click App information – Configure.
8. In the App information panel, click OK.
9. Click Add.
10. In the Slack panel, click Assignments.
11. In the Assignments panel, click Select Groups.
12. In the Select groups panel, use the search bar to find and select the iOSTest group. Click Select.
13. For iOSTest group, select Available for type, and click save.

Deploying a public Windows application

1. Browse to https://www.microsoft.com/en-us/store/p/slack/9wzdncrdk3wp, and copy the URL.
2. On the Azure Portal, select the Intune workspace.
3. In the Intune Workspace, select Mobile Apps.
4. In the Mobile apps panel, select Apps.
5. In the Apps panel, click Add.
6. In the Add app panel, for App type, select Windows store app. Click Configure.
7. In the App information panel, enter the following information:
   a. Name: `Slack`
   b. Description: `Slack`
   c. Publisher: `Slack Technologies, Inc.`
   d. Appstore URL: `https://www.microsoft.com/en-us/store/p/slack/9wzdncrdk3wp`
8. Click OK.
9. Click Add.
10. On the Slack panel, click Assignments.
11. On the Assignments Panel, click Select groups to include.
12. In the Select groups panel, use the search bar to find and select the WindowsTest group. Click Select.
13. For WindowsTest, for type, select Available. Click Save.

Deploying a web app

1. On the Azure Portal, select the Intune Workspace.
2. Select Mobile apps, then Apps.
3. Click Add.
4. In the Add app panel, for app, select Web app.
5. Click App information - Configure.
6. In the App information panel, enter the following information:
    a. Name: `Business Communication for Teams`
    b. Description: `Slack`
    c. Publisher: `Slack`
    d. App URL: `https://itunes.apple.com/us/app/slack/id803453959?mt=12`
7. Click Add.
8. In the Slack panel, click Assignments.
9. In the Assignments panel, click Select Groups.
10. In the Select groups panel, use the search bar to find and select the WindowsTest group. Click Select.
11. In the Assignments panel, for appletest group, for type, select Available, and click save.

Deploying profiles

Workspace ONE

Deploying a Profile to Android for Work

1. In the AirWatch console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, then Add Profile.
4. On the Add Profile screen, select Android.
5. On the Configuration Type screen, select Android for Work.
6. On the Add a New Android Profile screen, for Name, type `Android Password`. Under Assigned groups, select AndroidTest. Click Passcode.
7. Click Configure.
8. On the Passcode screen, for Minimum Passcode Length, select 6. Click Save and Publish.
9. On the Device Assignment screen, click Publish.

Deploying a profile to Apple iOS

1. In the AirWatch console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, then Add Profile.
4. On the Add Profile screen, select iOS.
5. On the Add a New Apple iOS Profile screen, for Name, type `iOS Password`. Under Assigned groups, select iOSTest. Click Passcode.
6. Click Configure.
7. On the Passcode screen, check the box to Require passcode on device. For Minimum Passcode Length, select 6. Click Save and Publish.
8. On the Device Assignment screen, click Publish.

Deploying a profile to macOS

1. In the AirWatch console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, then Add Profile.
4. On the Add Profile screen, select Device Profile.
5. On the Add a New Apple macOS Profile screen, for Name, type `macOS Password`. Under Assigned groups, select macOSTest. Click Passcode.
6. Click Configure.
7. On the Passcode screen, check the box to Require passcode on device. For Minimum Passcode Length, select 6. Click Save and Publish.
8. On the Device Assignment screen, click Publish.

Deploying a profile to Windows 10

1. In the AirWatch console, click Devices.
2. In the Devices workspace, under Profiles & Resources, select Profiles.
3. Click Add, then Add Profile.

4. On the Add Profile screen, select Windows.
5. On the Select Device Type screen, select Windows Desktop.
6. On the Add a New Windows Profile screen, for Name, type `Windows Password`. Under Assigned groups, select WindowsTest. Click Passcode.
7. Click Configure.
8. On the Passcode screen, for Minimum Passcode Length, enter 6. Click Save and Publish.
9. On the Device Assignment screen, click Publish.

EM+S

Deploying a profile to Android for Work

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune workspace, click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
    a. Name: Android Password
    b. Platform: Android for Work
6. Click Configure.
7. On the Android for Work compliance policy panel, select System Security.
8. On the System Security panel, select Required. For Minimum password length, enter 6. Click OK.
9. Click OK, then Create.
10. On the Windows Password panel, click Assignments.
11. On the Assignments Panel, click Select groups to include.
12. On the Select groups to Include panel, select AndroidTest, and click Select.
13. Click Save.

Deploying a profile to Apple iOS

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune workspace, click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
    a. Name: iOS Password
    b. Platform: iOS
6. Click Configure.
7. On the iOS compliance policy panel, click System Security.
8. On the System Security panel, select Required. For Minimum password length, enter 6. Click OK.
9. Click OK, then Create.
10. On the Windows Password panel, click Assignments.
11. On the Assignments Panel, click Select groups to include.
12. On the Select groups to Include panel, select iOSTest, and click Select.
13. Click Save.

Deploying a profile to macOS

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune workspace, click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
    a. Name: macOS Password
    b. Platform: macOS - PREVIEW
6. Click Configure.
7. On the Mac compliance policy panel, select System Security.
8. On the System Security panel, select Required. For Minimum password length, enter 6. Click OK.
9. Click OK, then Create.
10. On the Windows Password panel, click Assignments.

11. On the Assignments Panel, click Select groups to include.
12. On the Select groups to Include panel, select macOSTest, and click Select.
13. Click Save.

Deploying a profile to Windows 10

1. On the Azure Portal, select the Intune Workspace.
2. In the Intune workspace, click Device configuration.
3. On the Device configuration panel, click Profiles.
4. In the Profiles panel, click Create Profile.
5. On the Create Profile panel, enter the following:
    a. Name: Windows Password
    b. Platform: Windows 10 and later
6. Click Configure.
7. On the Windows 10 compliance policy panel, select System Security.
8. On the Password panel, select Required. For Minimum password length, enter 6. Click OK.
9. Click OK, then Create.
10. On the Windows Password panel, click Assignments.
11. On the Assignments Panel, click Select groups to include.
12. On the Select groups to Include panel, select WindowsTest, and click Select.
13. Click Save.

Appendix C: Test results

The following table breaks down the processes by task for our quantitative scenario.

Tasks	Workspace ONE		EM+S	
	Time (hh:mm:ss)	Steps	Time (hh:mm:ss)	Steps
Set up an organization				
Request the trial	0:00:41	2	0:01:28	6
Initial login	0:01:06	7	0:01:50	8
Configure and Install the software for the Enterprise Connector	0:01:14	9	0:02:13	20
Install the Enterprise Connector	0:02:06	20	0:03:47	18
Configuring Apple Push Notification Service for Apple Enrollment	0:02:21	24	0:06:21	24
Setup Android for Work	0:00:41	11	0:00:30	9
Email configuration	0:00:20	5	0:00:00	0
Set up users				
Create four new users separately	0:02:04	16	0:03:36	56
Create a new smart group	0:00:22	4	0:00:43	6
Enroll devices				
Enroll an iOS device	0:01:46	17	0:02:40	18
Enroll an Android device	0:02:43	18	0:02:52	19
Enroll a macOS device	0:02:04	21	0:01:07	10
Enroll a Windows 10 device	0:01:43	17	0:01:36	16
Deploy apps				
Deploy an internal application (Android, iOS, Windows 10)	0:00:51	9	0:01:42	14
Deploy an internal macOS application[2]	0:01:55	22	N/A	N/A
Deploy a public Android application	0:00:46	10	0:01:14	16
Deploy a public Apple iOS application	0:00:30	7	0:00:53	13
Deploy a public Windows 10 application	0:00:29	7	0:00:58	12
Distribute a web app	0:00:30	8	0:00:46	11
Deploy profiles				
Deploy a profile to Android	0:00:30	9	0:00:43	12
Deploy a profile to Apple iOS	0:00:29	8	0:00:45	12
Deploy a profile to macOS	0:00:29	8	0:00:44	12
Deploy a profile to Windows 10	0:00:31	9	0:00:44	12

Tasks	Workspace ONE		EM+S	
	Time (hh:mm:ss)	Steps	Time (hh:mm:ss)	Steps
Totals				
Set up an organization total	0:08:29	78	0:16:09	85
Set up users total	0:02:26	20	0:04:19	62
Enroll devices total	0:08:16	73	0:08:15	63
Deploy apps total[3]	0:03:06	41	0:05:33	66
Deploy profiles total	0:02:00	34	0:02:56	48
Scenario Total	0:24:16	246	0:37:12	324

[1] Intune does not have an internal catalog available to download and install for macOS. This results in a shorter enrollment time.

[2] Intune cannot deploy internal applications to macOS, therefore they cannot complete this task. We did not count the time to deploy macOS applications for either solution.

[3] We did not include "Support internal macOS application deployment" in our total time to deploy applications because Intune does not support it.

We captured responsiveness of each UEM solution by issuing a lock screen command to a managed iPhone. We started the timer as we issued the command and stopped the timer when we saw the device respond.

Response Time Data	Workspace ONE	EM+S
	Time (seconds)	Time (seconds)
Mean	1.455	18.78
Median	1.545	19.465
Min	1.11	5.75
Max	1.63	33.09

This project was commissioned by VMware.

Principled Technologies®

Facts matter.®

DISCLAIMER OF WARRANTIES; LIMITATION OF LIABILITY:
Principled Technologies, Inc. has made reasonable efforts to ensure the accuracy and validity of its testing, however, Principled Technologies, Inc. specifically disclaims any warranty, expressed or implied, relating to the test results and analysis, their accuracy, completeness or quality, including any implied warranty of fitness for any particular purpose. All persons or entities relying on the results of any testing do so at their own risk, and agree that Principled Technologies, Inc., its employees and its subcontractors shall have no liability whatsoever from any claim of loss or damage on account of any alleged error or defect in any testing procedure or result.

In no event shall Principled Technologies, Inc. be liable for indirect, special, incidental, or consequential damages in connection with its testing, even if advised of the possibility of such damages. In no event shall Principled Technologies, Inc.'s liability, including for direct damages, exceed the amounts paid in connection with Principled Technologies, Inc.'s testing. Customer's sole and exclusive remedies are as set forth herein.