How to Assess Windows Autopilot for Device Provisioning

Published 9 November 2021 - ID G00750386 - 18 min read

By Analyst(s): Eric Grenier

Initiatives: Collaboration and End-User Technologies for Technical Professionals

Windows Autopilot offers modern management-based provisioning for Microsoft Windows 10 and 11. Successful implementation demands understanding of its strengths and weaknesses. This research will help IT technical professionals avoid common pitfalls when implementing a Windows Autopilot program.

Overview

Key Findings

- Windows Autopilot is an enrollment tool, not an application deployment tool. Applications that require or force reboots will cause the Autopilot process to fail.

- Autopilot is a function of Windows and not dependent on the use of Microsoft Endpoint Manager (MEM). It can be used with any unified endpoint management (UEM) or mobile device management (MDM) solution.

- Not every use case is suitable for Autopilot. Desktops that will remain on the company network are not suitable for Windows Autopilot. Additionally, Windows Autopilot is not currently available for Government Cloud Community (GCC) High or Department of Defense (DoD) environments.

- Using hybrid Azure Active Directory (Azure AD) domain-join significantly complicates automated device enrollment with Autopilot and increases the likelihood of failure.

Recommendations

IT technical professionals responsible for end-user technologies should do the following when enrolling and provisioning Windows devices should:

- Utilize Windows Autopilot as a first step into modern management, and avoid hybrid-join scenarios.
- Make use of Windows Autopilot for automated device enrollment, and use your UEM platform to deploy applications after users log into their devices.
- Utilize your OEM/value-added reseller's preprovisioning services to configure devices with essential applications and settings. This is especially important for low-bandwidth situations.
- Simplify PC refresh and enable the use of Windows reset for break-fix by implementing cloud syncing of user data.

Analysis

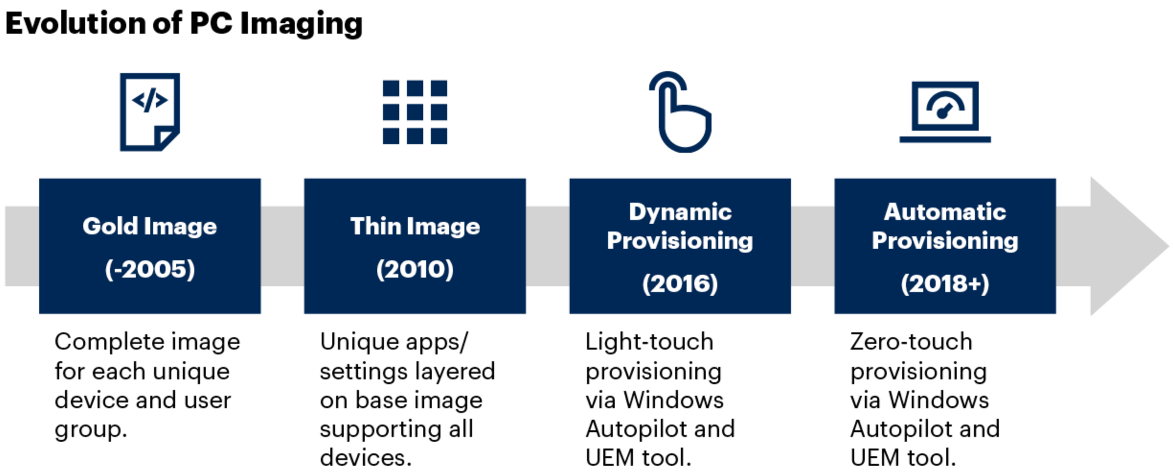
What Is Windows Autopilot?

Windows Autopilot is an automated device enrollment service for Windows 10 and 11 that allows you to automatically enroll Windows devices into your UEM platform. (Note that UEM includes mobile device management [MDM] functionality.)

Autopilot is often mistakenly thought to require Microsoft Endpoint Manager (including Microsoft Intune), but Autopilot is a function of Windows, not the management platform. Registering and automating device enrollment for Windows devices via Autopilot is similar to registering and enrolling devices in Apple Business Manager (formerly DEP) and Android zero-touch enrollment (ZTE).

The process to move a device from an OEM to a business-ready state has gone through many evolutions and, with the introduction of modern management, Autopilot has become an essential tool for device provisioning (see Figure 1).

Figure 1: Evolution of PC Imaging

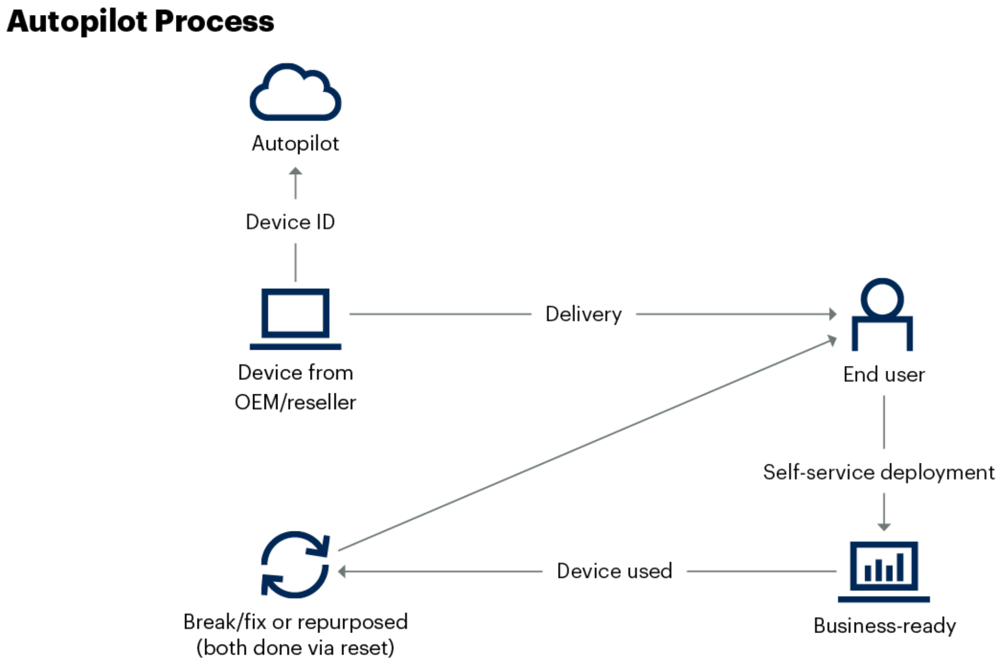

Evolution of PC Imaging
Gold Image (-2005)
Thin Image (2010)
Dynamic Provisioning (2016)
Automatic Provisioning (2018+)
Complete image for each unique device and user group.
Unique apps/ settings layered on base image supporting all devices.
Light-touch provisioning via Windows Autopilot and UEM tool.
Zero-touch provisioning via Windows Autopilot and UEM tool.

Source: Gartner
723476_C

Autopilot’s primary purpose is to get a device activated and enrolled. Getting the user to the desktop as quickly as possible, and then allowing your UEM platform to take over the provisioning and configuration of the device, is critical to minimizing wait time (see Figure 2). Autopilot can improve the user experience, when compared with previous provisioning mechanisms, as it minimizes the time spent in waiting screens. When users have to wait extended periods to get to their desktop, this often leads to unnecessary calls to the help desk because the users are unsure what is happening on their device.

Although Autopilot can be used as an imaging/provisioning/configuration tool, Gartner does not consider Autopilot alone to be sufficient for managing endpoints.

Figure 2: Autopilot Process



Source: Gartner
750386_C

Licensing Prerequisites

The following licensing prerequisites exist for using Autopilot:

- A supported version of Windows 10 or Windows 11 Pro, Enterprise, or Education (Home edition is not supported).
- An Azure Active Directory P1 or P2 license.

Integrate Azure AD With Your UEM Platform

Integrate Azure AD with your UEM platform before setting up your Autopilot profiles. If you are using MEM/Intune as your platform, this is not required as the integration piece is established by default. For all other UEM platforms, you will have to connect your UEM platform to your Azure AD (refer to the vendor documentation for your platform for details of how to do this). Along with the Azure AD connector for your platform, you will need to configure all users to have permission to join devices to Azure AD.

Populate Devices Into Autopilot

Devices can be added to Autopilot in two ways. Your OEM or value-added reseller (VAR) can add hardware hashes to Autopilot before shipping. This may be offered as an included service or as a service for which you pay an additional charge. Alternatively, devices can be manually added via a PowerShell script. To do so, a PowerShell script must be executed from a command prompt on the endpoint being added, before going through the Out of Box Experience (OOBE), if it is a new device. The results need to be exported to a .csv file, which must then be uploaded to Microsoft Endpoint Manager.

Gartner recommends using OEMs/VARs to add devices to Autopilot. This is more reliable and convenient than PowerShell scripting, and is done before the devices ship. This requires you to give your OEM/VAR authorization to populate your tenant with devices. Global Administrative privileges are required in order to provide that authorization.

Gartner recommends using the PowerShell script approach only when adding existing devices retroactively to Autopilot. You will then be able to utilize Windows reset to easily repurpose machines by factory resetting them and going through the Autopilot process. This will also assist IT staff when they need to perform break/fix functions by allowing devices to revert easily to a known state without having to touch them.

Device Prerequisites

The following device prerequisites exist for successful Autopilot setup:

- **Internet access on the device being provisioned.** The best user experience occurs when the device is directly connected to an Ethernet port rather than connected via Wi-Fi. Provisioning can still happen over Wi-Fi, but the customized OOBE does not happen until the user manually makes the Wi-Fi connection. If the user hardwires the device before powering on, they get the exact experience that you have customized for them immediately.

- **Populate devices into Autopilot.** Only PCs that are registered to your tenant will be able to receive the Autopilot configuration profile that you deploy for your Windows 10 or 11 devices.

- **Trusted Platform Module (TPM) 2.0 and TPM attestation support.** Devices need to have TPM 2.0, which might require a firmware upgrade (please check with your OEM). The TPM also needs to support attestation. Autopilot will fail if this requirement is not met.

For a full list of requirements, click the links below:

- Windows Autopilot software requirements
- Windows Autopilot configuration requirements
- Windows Autopilot networking requirements
- Windows Autopilot licensing requirements

Common Pitfalls of Autopilot

Optimal Windows Autopilot deployments enroll devices into your UEM platform and then allow UEM to take care of the software deployment and device configurations required by your organization after the user logs into the device. Autopilot deployments may fail when the following scenarios apply:

- **Deployment of too many applications:** Autopilot is an enrollment tool, not an application deployment tool. Applications that require or force reboots will make the Autopilot process fail. Trying to deploy applications other than a web browser and a deployment package that configures the UI (start menu customization, screen saver, desktop background and so on) during the Autopilot process will delay end users getting to the desktop. Bandwidth is an issue for remote workers; their connections tend not to be as fast as the company network, and the slower the connection is, the longer it will take to push the applications to the device.
    - **How to avoid this pitfall:** Divide your application portfolio into “first-day” and “not first-day” applications. Have your OEM/VAR preprovision devices with “first-day” applications before shipping to your end users. Alternatively, use your UEM platform to provision “not first-day” applications after the user’s first login is complete.

- **Deployment of security settings and configurations during the Autopilot process:** Security software and configurations that touch the kernel can prevent or inhibit network access and cause the Autopilot process to fail.

    - Examples of security and configurations and security software to avoid during Autopilot include:

        - **BitLocker encryption:** This requires a reboot and will cause the Autopilot process to fail. In addition to the reboot, your user will have to wait hours for encryption to occur before being able to get to their desktop. Encryption can occur after login.

        - **Network proxy:** A clean network connection is essential to a successful Autopilot process, and network proxies can filter data that is needed for Autopilot to complete successfully.

        - **Other agents:** For instance, endpoint protection, endpoint detection and response, and secure web gateways that force a reboot.

    - These are things that touch the kernel, prevent or inhibit network access. Configure your management tool to deploy your security software and configurations *after* the user gets to the desktop.

    - **How to avoid this pitfall:** Have your OEM/VAR preprovision security software and configurations before shipping devices to your organization or the end users. This will enable the devices to be minimally protected and you to make user-specific configurations after initial login.

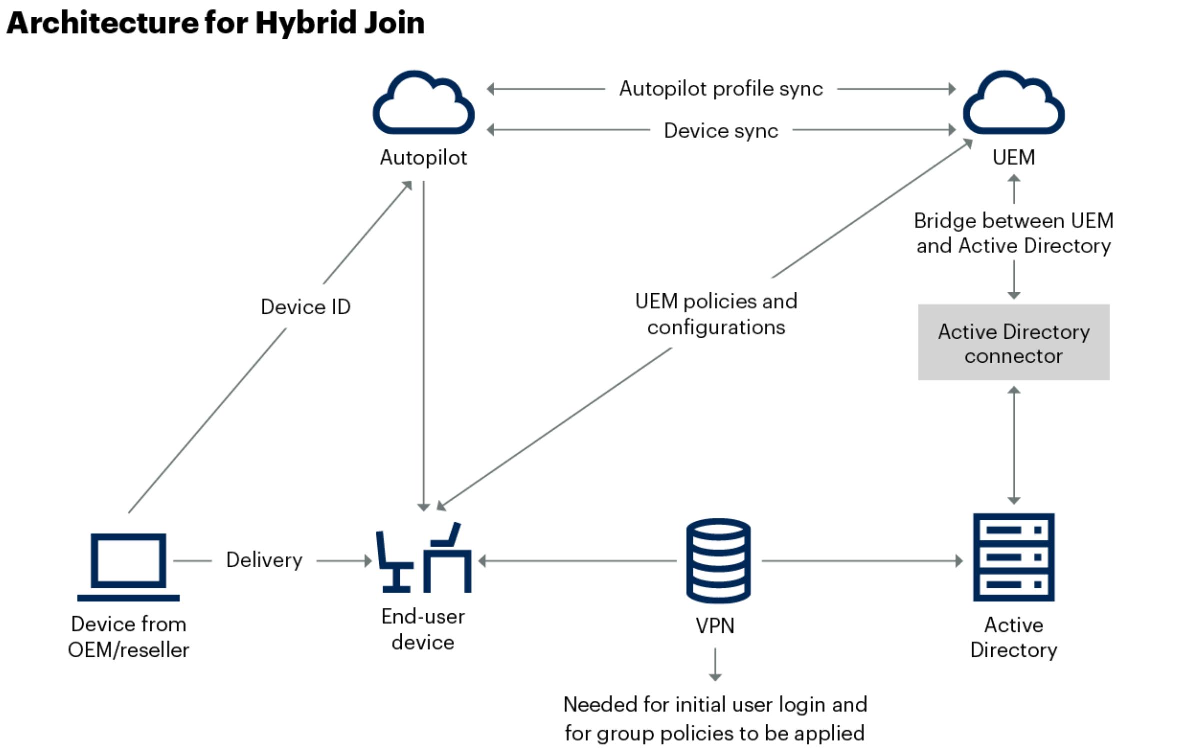
        - Preprovisioning only the essential settings is necessary because UEM/MDM platforms do not allow you to prioritize specific configurations and settings over others — they get set randomly.

        - Gartner does not recommend using internal IT staff to preprovision devices, unless it is absolutely necessary. Using internal IT staff will increase shipping costs and the time it takes to get the device to the end user.

        - If you are shipping every device to headquarters, so that internal staff can touch them and then ship them to end users, you are losing one of the main benefits of an Autopilot program.

- **Hybrid domain-join scenarios:** Autopilot offers the ability to hybrid-join devices to your on-premises AD as well as your Azure AD, but adds significant complexity to the process. You have to install a UEM connector to your traditional AD domain controller to enable on-premises domain join for remote devices. Not all UEM platforms have a connector.
  - **How to avoid this pitfall:** This is straightforward if the UEM platform supports this scenario. But for a user to log into the device the first time, you need to have Start Before Login VPN enabled or Always-on VPN enabled, neither of which are supported by all VPN applications (see Figure 3).

Figure 3: Architecture for Hybrid Join


Architecture for Hybrid Join
Autopilot profile sync
Device sync
Autopilot
UEM
Bridge between UEM and Active Directory
Device ID
UEM policies and configurations
Active Directory connector
Delivery
Device from OEM/reseller
End-user device
VPN
Active Directory
Needed for initial user login and for group policies to be applied

Source: Gartner
750386_C

Strengths

Windows Autopilot provides the ability to significantly reduce deployment time and effort for mobile Windows devices. The strengths of an Autopilot approach include:

- **Creation of a clean slate for configuration and management.** Using Autopilot to move to modern management creates a clean slate — old and outmoded settings can be left behind. Moving to policy-based management allows the registry to stay clean and provides full management from any internet connection.

- **Reduced time-to-use.** Through the use of "user-driven" mode in Autopilot, devices can be shipped directly to end users. They can walk through the steps to provision the device automatically, thus reducing the time that IT staff need to spend on these tasks and giving them more time to focus on critical activities.

- **Enabling of preprovisioned deployments.** Through the use of "preprovisioned" mode in Autopilot, organizations can have OEMs/VARs provision devices with applications and configurations before shipping to the end user, so that the end user spends less time waiting for the processes to finish. Preprovisioning can be done by on-site IT staff as well, but this will increase the time taken to get the device to the end user, and will add extra shipping costs to the process.

- **Enabling of automatic enrollment.** Autopilot leads to consistent enrollment and prevents any worrying about getting devices enrolled manually or through discovery. Enrollment happens automatically as long as the device has successfully connected to the internet during the OOBE.

Weaknesses

Windows Autopilot represents a big change when compared with the traditional imaging and delivery of mobile Windows devices. Weaknesses of an Autopilot deployment include:

- **Potential for complexity with the use of hybrid Azure AD domain-join scenarios.** Autopilot offers the ability to hybrid-join devices to your on-premises AD, as well as to your Azure AD, but this adds complexity to the process. You will have to install a connector from your UEM platform (if one is available — not all platforms have a connector, so please check with your vendor) that will allow you to join the device to the domain without the device being on the company network. This is straightforward *if* the vendor supports this scenario, but in order for a user to log into the device, you will need to have Start Before Login VPN enabled or Always-on VPN enabled.

- **Degraded experience in low-bandwidth situations.** Autopilot processes will be at the mercy of the user's internet speed at the time of setup. A user with a slower internet connection will have a degraded experience. Preprovisioning will help compensate for slow connection speeds.

- **Dependence on cloud resource availability.** You are dependent on the cloud resources being available at the time of deployment/enrollment/configuration. Autopilot is dependent on Azure AD and Microsoft Endpoint Manager being available. If either service is down during the Autopilot process, users will not be able to enroll their devices and/or login. Since January 2020, the Azure AD service has gone down five times; sometimes for as little as 20 minutes, but also for as long as 14 or more hours. (For more information, see How to Mitigate the Impact of Microsoft 365 Downtime.)

- **Inability to have UEM deployment prioritization.** UEM platforms do not offer the ability to prioritize the order in which deployments of applications and configurations occur. This can cause challenges with applications that have other software dependencies. To minimize the impact, use OEM/VAR preprovisioning, whenever possible, so that when the user receives the device it is already configured with the foundational applications and security configurations required by your organization.

Guidance

Windows Autopilot can be an efficient way to get devices automatically enrolled into your UEM platform. However, if the Autopilot process is designed to do more with Autopilot than was intended, this can result in a poor end-user experience. The user experience needs to be paramount whenever you are designing Autopilot deployments.

Make Modern Endpoint Management Part of Your Roadmap

Autopilot is a tool to enroll devices automatically into modern endpoint management solutions and should only be used when that approach is part of your organization's roadmap and strategy. If your endpoint management strategy is to stick with legacy configuration management tools (CMTs), Autopilot is not recommended. Although Autopilot does support hybrid environments, they add unnecessary complexity and can often lead to failure during the Autopilot process.

Examples of this complexity include:

- The need for Always-on VPN or Start Before Login VPN

- The need for an AD connector to perform the machine domain join

- The need to install the agent for your on-premises endpoint management tool and, if co-management is being used, to ensure machines are properly managed

Take the opportunity to create a “green field” for modern managed devices. Do not spend time matching Group Policy Objects (GPOs) to policies. Instead, create your desired device posture and match that to the policies available in your UEM platform.

Hybrid environments represent a delaying, “kick the can down the road” approach to endpoint management that allows organizations to bring along years’ worth of technical debt. In some scenarios, such as where there is a high dependency on application-specific GPOs, or where security controls require a VPN, this approach is unavoidable. Ideally, Autopilot should serve as an enrollment tool for your UEM platform, which is a modern management tool.

You should:

- Choose an OEM/VAR that supports Autopilot registration.
- Select a UEM platform that supports a connection with Azure AD.

Configure Autopilot for a Streamlined and Effective IT Process

Creation of Autopilot Profiles

Do not use the Microsoft Store to create Autopilot profiles as it lacks feature parity with Microsoft Endpoint Manager (MEM). Instead, create your Autopilot profiles in MEM, even if you are using another UEM platform. Please note: If you only have Azure AD P1 or P2 (without a Microsoft Intune subscription), you will only be able to create Autopilot profiles in the Microsoft Store, as an Intune service principal is required to create profiles in MEM. An Intune service principal is included with the following subscriptions:

- Microsoft 365 Business Premium
- Microsoft 365 F1 or F3
- Microsoft 365 Academic A1, A3, or A5
- Microsoft 365 Enterprise E3 or E5
- Enterprise Mobility + Security E3 or E5
- Intune for Education

Use Dynamic Device Groups

Autopilot profiles need to be assigned to Azure AD groups. There are many queries to create dynamic groups based on users or devices (you cannot create device groups based on user attributes or vice versa). The most efficient way to create a dynamic device group is to target all Autopilot devices using the following query: (device.devicePhysicalIDs -any (_ -contains “[ZTDId]”))

Use Autopilot to Automatically Name Devices Based on Your Naming Convention

Your Autopilot profile should be configured to name devices automatically, based on your organization’s naming convention. This ensures that standards are followed and avoids it having to be done manually by IT staff or end users.

Connect Your UEM Platform to Azure AD for Automatic Enrollment

Autopilot is a tool for getting devices enrolled. To ensure enrollment happens automatically, you will need to connect your UEM platform to Azure AD. This is done in the Mobility (MDM and MAM) blade within Azure AD.

Utilize Your Cloud Sync Tools to Sync User Profiles and Documents

User profile and document transfer is a significant challenge with PC refreshes. Utilize your organization’s cloud storage services (OneDrive for Business, Box, Dropbox, Citrix ShareFile and others) to make this process more efficient and eliminate the manual effort needed to transfer files to the new device. Turning on Enterprise State Roaming in Azure AD will assist with the user profile synchronization, which is available to all Azure AD Premium customers.

Make the Process Simpler and Faster for End Users

Use Company Branding for the OOBE Screen

Before creating your Autopilot profile in MEM, take the time to customize your OOBE. This will provide end users with an experience that has familiar company branding at the very beginning. The idea here is to set the user’s mind at ease. This is done in the Azure AD portal in the Company Branding blade.

Gartner recommends customizing the following options, at minimum:

- Sign-in page background image
- Banner logo
- Sign-in page background color

- Square logo image
- Square logo image, dark theme

Create an On-Brand UI Deployment Package

This package will make changes that are on-brand with your organization. Among other things, you should at least change:

- Desktop background
- Start menu customization
- Screensaver
- Power settings

Avoid Installing Applications That Have Dependencies or That Will Cause a Reboot

Autopilot should be used as a tool for enrollment. Autopilot struggles when applications that require a reboot are installed. Autopilot cannot keep track of enrollment or installations when a restart occurs before enrollment — Autopilot fails and the device will need to be reset. Organizations can use preprovisioned Autopilot for preprovisioned deployment to eliminate the need to install anything during the Autopilot process:

- Organizations can have devices shipped to IT, where they can be provisioned and then shipped to users.
- Organizations can work with OEM/VARs to have devices preprovisioned and then shipped directly to the users.

Run Tests After Configuring All Settings to Ensure a Smooth Deployment

You want to make sure that the process goes smoothly and that you are testing every scenario in which Autopilot will be used. This includes testing all device types, device locations (home, office, public Wi-Fi) and user types (based on configuration profiles pushed to the devices by your UEM platform). Ensure that your Autopilot process works by running a series of tests.

Undertake the following tests, at minimum:

- Test for varying internet connection speeds and locations.

- Test for provisioning times for each of the scenarios.
- Test the OOBE.
- Test all Autopilot profiles.
- Test UEM deployment processes after initial logon.
- Ensure devices are enrolled into your UEM platform.
- Test Windows reset and Autopilot for reprovisioning existing devices.

Train Users to Use Self-Service Portals for Installation of Optional Software

Populate your self-service portals with applications that are not part of your foundational configuration. After doing so, train your end users to access the self-service portal and install applications necessary for their specific jobs. This will reduce the burden on the UEM tool and give users a sense of empowerment over the management of their devices.

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

Magic Quadrant for Unified Endpoint Management Tools

Critical Capabilities for Unified Endpoint Management Tools

Advance and Improve Your Mobile Security Strategy

Embrace Windows 10 Modern Management to Enable a Highly Distributed Digital Workplace

How to Implement Continuous Endpoint Engineering: An Agile Approach for the Digital Workplace