PIQUE SOLUTIONS

Device and Application Management: Windows 10 versus macOS High Sierra and iOS 11

Manageability Feature and Functionality Comparison

PIQUE SOLUTIONS

April 2018

THE DEVELOPMENT OF THIS WHITE PAPER WAS SPONSORED BY MICROSOFT. THE UNDERLYING RESEARCH AND ANALYSIS WERE EXECUTED INDEPENDENTLY BY PIQUE SOLUTIONS.

795 Folsom Street, 1st Floor | San Francisco, CA 94107 | Tel.: 415.685.3392 | www.piquesolutions.com

Contents

Pique Solutions is a competitive research and market analysis firm supporting Fortune-500 companies in the information technology sector. Pique is based in San Francisco, California.

Executive Summary

Based on in-depth review of product documentation and hands-on testing, Pique Solutions conducted a comparative analysis of the management capabilities of Microsoft Windows 10 and Apple macOS High Sierra and iOS. The analysis assessed the level of functionality those capabilities provide, the utility of those capabilities, and their impact on user experience.

Enterprise networks are comprised of a mixture of device types, with most employees having access to enterprise information on both their personal and work systems. To manage this complex environment, enterprises must govern the flow of data that progresses across both corporate and personal devices and applications. Managing devices and applications is a complex task for enterprises as they try to ensure that employees have secure access to relevant enterprise data while retaining the privacy of their personal data.

Based on extensive analysis of all three platforms, Pique Solutions concluded that Microsoft provides a more comprehensive and usable set of management capabilities and tools for managing and securing devices when compared to Apple. Microsoft's modern management solution, Microsoft Enterprise Mobility + Security (EMS), provides a more comprehensive set of native controls for enrollment, policy, patch, compliance, and application management. While macOS and iOS can achieve similar management capabilities, third-party tools for management and provisioning are needed to achieve functional equivalence with EMS, along with the purchase of a server application add-on that runs as additional service with various subcomponents.

macOS supports provisioning packages for use with the provisioning profile and configuration tools. It also includes cryptographic signing and encryption of provisioning packages with password-based user access to configure email and other user accounts, including corporate iCloud accounts, which require authorization to purchase software from the Apple Store. Pique Solutions learned that macOS supports configuration of account payloads with user name, email address, certificate identities for authentication, and signing. However, to achieve parity with Windows 10 single-step mobile device management (MDM) discovery, provisioning, and enrollment, macOS requires the use of Microsoft Certificate Authority using DCE/RPC and the Active Directory Certificate profile payload and AD authentication.

Last, Pique Solutions found that while macOS and iOS provide a robust method for application and software distribution, they require the use of Apple Store for distribution of purchased software and for whitelisting of applications. This requires the enterprise to purchase a license to register corporate devices. In comparison, Windows 10 supports software distribution through multiple methods with no additional costs incurred.

Introduction to Device Management

Unlike the mobile space where using personally owned devices for work is becoming more common, desktops are usually company-owned and -managed. Laptops are a combination of the two, with a growing proportion of personally owned devices being used for business. Even within those broad categories, device and application management requirements vary widely among organizations. While some might require a light level of management, others need very granular controls to protect sensitive corporate data.

Microsoft has a long history of managing desktop and laptop computers and tablet PCs with very detailed controls in System Center Configuration Manager (SCCM), with capabilities that are relatively new in the macOS environment.

Windows-based devices have long offered efficient management capabilities, and that legacy continues with Windows 10. Apple added API-based management to macOS in 2011 with the release of Lion (macOS 10.7), and Microsoft followed suit with Windows 10. The management APIs are built into Windows 10, and a download is available to allow macOS devices to be supported by System Center Configuration Manager.

In addition, Microsoft provides deep manageability and security functionality through technologies like Azure AD, Intune, and Group Policy, all of which can be administrated through the Azure-based portal in EMS. This significantly streamlines management of workflows in those solutions. For “mobile-first, cloud-first” environments, Microsoft provides a simplified modern management solution using cloud-based device management tools in the Microsoft Enterprise Mobility Suite. These capabilities are complemented by cloud services like Microsoft Intune, Azure AD, Azure Rights Management Service, Office 365, Azure Information Protection, and Windows Store for Business. With these unified tools, enterprises can manage devices, users, and groups with nearly unlimited scale. Today’s complex device landscape presents an array of challenges to keep data secure on corporate-owned, employee-owned, and foreign-owned devices. Microsoft Intune manages this complexity by providing robust capabilities for device management, application management, or a combination of the two, depending on specific needs.

While MDM tools are often a requirement for many cross-pollinated solutions by Microsoft with Apple mobile devices, technology and mindsets of the past—requiring multiple toolsets and products to manage both environments—are still prevalent in the enterprise today. The reliance on third-party MDM tools, however, is decreasing as OS vendors improve the functionality of their own management solutions.

Assessment Methodology

The overall assessment methodology developed by Pique Solutions was as follows:

1. Based on product documentation and hands-on testing, we determined the management features and capabilities provided natively across Microsoft Windows 10, Apple macOS (High Sierra), and Apple iOS 11. Additionally, for those platforms that are unable to address the features natively, we identified and assessed the functionality of third-party tools needed to supplement the native functions.

2. We conducted interviews with subject matter experts to verify assumptions and platform capabilities.

3. The comparison of Apple's and Microsoft's management features and functionality was based primarily on publicly available product documentation and other relevant public data.

4. When public data was not available or was not sufficient, hands-on testing was conducted to compare specific features or functionality.

When scoring the relative feature and functionality of the three platforms, Pique Solutions applied the following scoring methodology. The baseline was calculated as the maximum score attainable, multiplied by the number of features evaluated in each category.

Feature	Functionality
1 - Requires 3rd-Party SW	1 - Not Intuitive
3 - 25% Integrated	3 - Slightly Intuitive
6 - 50% Integrated	6 - Moderately Intuitive
9 - 100% Integrated	9 - Highly Intuitive

To assess Windows 10, macOS, and iOS 11, Pique Solutions researched the features and functionality across five main categories:

- **Device Enrollment:** Discovery, certificate, provisioning
- **Device Configuration and Policies Supported:** Network, device resources management, geo-fencing
- **App Management:** Delivery, update, configuration, app black-/whitelisting
- **Remote Assistance:** Asset management, OS and security updates, lost device, remote wipe
- **Monitoring:** Anomalous behavior detection, compliance, root detection

For the testing environment, we used the most widely adopted and common software in the enterprise market: Microsoft Windows Server, Microsoft Active Directory, Office 365 (documents and email), "Enterprise App" (a lightweight limited-functionality app to simulate an enterprise-provided app), "Personal App" (a lightweight limited-functionality app to simulate a personal app), and OneDrive. The MDM system used was EMS E5 integrated with a set of Microsoft tools, Apple apps, and ATA, DLP, and UBA.

Key Findings

Based on our comparative feature assessment of Windows 10, macOS, and iOS in the manageability category, Windows 10 provides a better solution than macOS and iOS for the enterprise. The following are the key differentiators that led us to that conclusion:

- Windows 10 offers single-step domain authentication, provisioning, and management.
- macOS provides flexibility to enhance functionality, but this is based on integration of third-party tools using Apple extension support; Apple will not act as a single source of support for these integrated tools beyond its own protocol.
- Windows 10 remote health attestation ensures device compliance. Conditional access limits exposure to devices that are not compliant.
- Windows 10 offers extensive patch management and reporting capability.
- macOS and iOS patch management requires patching and policy to occur in a hybrid cloud environment with dependencies on Apple servers.
- Windows 10 supports a broad range of management and configuration options for mixed hardware and operating system environments.
- Apple management servers are designed to support only Apple-specific devices.
- macOS and iOS lack the ability to control approved applications and restrict use of webcams and card readers.
- macOS devices use Simple Certificate Enrollment Protocol to create unique identity certificates for authenticating an organization's services.

Deploying and using device management platforms requires significant training, time, and resources. However, our analysis showed that Microsoft Enterprise Mobility + Security (EMS) and Windows AutoPilot significantly reduce the complexity and cost of provisioning and managing devices because most of the previously manual tasks are now fully automated and reimaging of devices is no longer necessary. Using a combination of these tools constitutes a scalable management platform that ties into existing user authentication and provisioning systems (e.g., Active Directory or a hybrid solution Azure Active Directory to fully facilitate cloud deployments) and provides automated device setup and configuration.

For personally enabled devices, EMS supports conditional access control policies for user access to enterprise resources. Users enroll their devices with EMS, which auto-provisions the device based on policy settings that provide organizational settings and apps over the air, along with application and geographical restrictions. For devices purchased directly from Apple or a device carrier, one can also take advantage of Microsoft Intune to automatically enroll new devices into the enterprise using EMS and put restrictions on the types of content available that a user can put on the mobile platform. This assures that when employees lose their device or leave the organization, they only leave with their device and personal data and not any sensitive corporate data. Our testing of this use case confirmed that EMS enforces settings, monitors corporate compliance, and removes corporate data and apps, while leaving personal data and apps on each user's device intact. For more information on EMS, see the Enterprise Management + Security website.

On configured devices, users are allowed personal applications and data in addition to corporate accounts and applications. Shared devices used for a single purpose are configured

and managed centrally rather than relying on user configuration. With a nonpersonalized device deployment, users are restricted from installing applications or storing personal data on a device. Beyond Windows 10 support, EMS supports the use of restrictive settings across multiple device platforms, including macOS and iOS.

Pique Solutions found that Apple offers limited native capabilities for managing and configuring macOS and iOS devices in a heterogeneous enterprise environment. In a more complex enterprise environment, an effective and secure management of Apple devices and applications requires the implementation of third-party MDM and Identity and Access Management (IAM) solutions. We determined that three distinct third-party tools are required for Apple to achieve parity in management functionality with Windows 10 with EMS.

Feature and Functionality Comparison

Device Enrollment

The table below summarizes the results of our hands-on testing of the device enrollment capabilities provided by Microsoft and Apple. Microsoft achieved the perfect score in all three categories (discovery, certificate, provisioning) while Apple performed worse in comparison, more notably for iOS.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**27**	**27**	**27**
macOS High Sierra	**27**	**20**	**12**
iOS	**27**	**13**	**9**

A few things should be mentioned before discussing device enrollment. There are several different types of device enrollment use cases: bring your own device (BYOD), corporate-owned device (COD), and device enrollment manager (DEM). An administrator is typically responsible for enrolling enterprise-owned devices before they are issued to the user.

- **Bring Your Own Device:** BYOD includes personal phones, tablets, and PCs. Users install and run the company portal app to enroll BYODs. This program lets users access company resources like email.
- **Corporate-Owned Device:** CODs include phones, tablets, and PCs owned by the organization and distributed to the workforce. COD enrollment supports scenarios like automatic enrollment, shared devices, and preauthorized enrollment requirements. A common way to enroll CODs is for an administrator or manager to use the DEM.
- **Device Enrollment Manager:** DEM is a special user account that allows enrollment and management of multiple CODs. Managers can install the company portal and enroll many userless devices.

Existing enterprise management tools, such as Group Policy Orchestrator (GPO), Windows Management Instrumentation (WMI), PowerShell scripts, and SCCM, continue to work for Windows 10, and there is now a built-in agent for joining Microsoft's own EMS management solution.

After enrolling in the program, administrators can log into the EMS website, link the device to their EMS servers, and assign devices to users. Once assigned, users can go through the Setup Assistant on their devices; any enterprise-specified configurations, restrictions, and controls are automatically installed.

When users enroll themselves into the EMS management solution by logging into a new or existing device with their Azure credentials and accepting the enterprise policy, their device is reconfigured with the settings approved and enforced by the enterprise. Some 400 common settings are available to the enterprise out-of-the-box, with support for additional PowerShell and WMI scripts that administrators can use to perform more granular settings, such as GPO security, network, hardware component restrictions, and the like.

Other methods of enrollment include conditional enrollment. This is an effective option for BYOD scenarios where employees and contractors use personal devices for business. The granular restrictions within conditional enrollment will ensure that when the employee or contractor leaves the organization, all email, contacts owned by the company, and business apps and data will be wiped.

EMS gives organizations the ability to securely enroll devices in the corporate environment, wirelessly configure and update settings, monitor policy compliance, deploy apps and books, and remotely wipe or lock managed devices. This is not limited to Windows 10 devices, as EMS can also be used to manage Android-, iOS-, and macOS-based devices.

In addition, Microsoft recently introduced a game-changing management tool, Windows AutoPilot. With AutoPilot, a user can take delivery of a new Windows 10 device straight from the vendor and the device will provision itself in a matter of minutes. The combination of EMS and AutoPilot provides unparalleled device enrollment capabilities especially to enterprises adopting the modern management principles empowered by the cloud. (To learn more about enrolling and configuring Windows devices using AutoPilot, refer to the Windows AutoPilot Deployment Program website.) For those organizations that are yet to make that transition, Microsoft is developing processes to assist customers who currently do not utilize any cloud services but are interested in a shift to modern management. For example, co-management is a new concept that allows Windows 10 devices to be managed by Microsoft Intune MDM and the SCCM agent at the same time. It will provide a mechanism for organizations to migrate workloads to modern management at their preferred pace. A variety of third-party MDM solutions are available to support different server platforms. Each solution offers different management consoles, features, and pricing.

EMS provides a fast, streamlined way to deploy enterprise-owned devices, by using a simplified initial setup that automates enrollment and the supervision of devices without having to physically touch or prepare them before users get them. This process can be made even simpler for users by removing specific steps in Setup Assistant, so users are up and running quickly, making the enrollment process quick and painless.

Auto-enroll and BYOD policies are very popular ways of enrolling devices and associating them with users when it comes to application management. Windows 10 enrollment can be performed using the auto-enroll or BYOD policies, although if an enterprise has several hundred or thousands of devices to enroll, bulk enrollment is always an option. Whether one is using the Azure-based auto-enrollment, bulk enrollment, or the Windows AutoPilot deployment program, numerous options and wizards are available for specific management requirements and device ecosystems.

The macOS native management platform is the on-premises solution of macOS Server 5.5 and AppleID for identity management. We found enrolling devices into the device manager to be much more time-consuming and cumbersome compared to Windows 10 and EMS. First, you must buy the server application from Apple. Any devices purchased outside of Apple need to be purchased through an approved partner at an undisclosed fee and the ResellerID needs to be provided. Apple allows the administrator to also manually add iOS devices to the Device Enrollment with Apple Configurator 2 (version 2.5 or later). The enrollment options for macOS are Forced Re-enrollment and Verified Access. These are the only options for enrolling Apple devices, and their capabilities are as follows.

Forced Re-enrollment

This setting forces a device to re-enroll into a domain after wiping by default. When this feature is disabled, the device is not forced to re-enroll after wiping. Once enabled, if the user does not want an Apple device to re-enroll in a domain, he or she needs to deprovision or disable the device. When the Forced Re-Enrollment device policy in the Admin console is turned on and the user wipes or recovers the device, the enrollment screen is the first thing the user sees when he or she restarts the device. This means that the user must re-enroll the device into a domain before using it. If the user does not re-enroll the device, he or she cannot sign in to it, browse in guest mode, or see the consumer sign-in screen.

Verified Access

The main features of verified access are the following:

- **Enable for Content Protection:** Ensures that Apple devices in your organization will verify their identity to content providers using a setting that enables a web service to request proof that its client is running an unmodified operating system that is policy-compliant.
- **Disable for Content Protection:** If disabled, some premium content may be unavailable to your users.
- **Enable for Enterprise Extensions:** Enables Verified Access for the devices in this organizational unit. If enabled, Apple extensions can interact with the Trusted Platform Module on the device.
- **Disable for Enterprise Extensions:** If disabled, Apple extensions attempting to perform Verified Access will receive a permissions error.

Verified access is how a network service, such as a VPN gateway, a sensitive server, an Enterprise certificate authority, or an Enterprise Wi-Fi access point can get a hardware-backed cryptographic guarantee of the identity of the device and the user trying to access it. Verified Access ensures that a device connecting to your network has been unmodified and is policy-compliant. Verified Access does not use a Trusted Platform Module to enable enterprise network services to cryptographically confirm the identity and status of verified boot and enterprise policy. Apple uses software keys and hashes via a web service request. The administrator needs to enable the Verified Access feature in the Apple Server console and force a web request to the user's Apple devices. Once this is done, the network service talks to the Verified Access Server API to determine the policy compliance and talks to Apple Server to (optionally) determine the identity of the client device. Service accounts that can receive a device ID will list email addresses of the service accounts that gain full access to the Apple Server Verified Access API. Service accounts that can verify a device but do not receive a device ID will list email addresses of the service accounts that gain limited access to the Apple Verified Access API. Most API access will need to be performed from the Server console.

Device Configuration

The following table summarizes the results of our hands-on testing of the device configuration capabilities provided by Microsoft and Apple. Microsoft, again, outperformed Apple in all four categories (network management, device policy, geo-fencing, remote wipe). Apple's largest

comparative weaknesses were found in the network management and geo-fencing categories for both Apple iOS and macOS High Sierra.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**36**	**36**
macOS High Sierra	**36**	**26**	**19**
iOS	**36**	**30**	**25**

Configuration profiles automate the management of settings, accounts, restrictions, and credentials. In Windows 10, they can be delivered through EMS if one needs to configure many devices and prefers a low-touch, over-the-air deployment. Profiles can also be sent as an email attachment, downloaded from a web page. These settings can also impose geo-fencing in regard to the types of service that will be available when an employee or contractor travels out of the country. Many enterprises have strict policies due to their industry affiliation that might require users to enroll in EMS to obtain access to email and contacts. This can be achieved by using the EMS solution to automatically administrate email configuration and contact synchronization. Once a device is enrolled, an administrator can approve the device or simply leave it to the system to identify the user via Azure ID and let the policy automatically flow down to the device. Then the device (Windows 10 or Apple iOS and macOS High Sierra) receives notification of the policy via an established secure communication, and the devices can receive EMS policy updates and remote commands anywhere in the world.

Most enterprise mobility management solutions support basic mobile device and mobile app technologies. These are usually tied to the device being enrolled in your organization's MDM solution. Microsoft Intune supports these scenarios and additionally supports many "without-enrollment" scenarios.

Organizations differ to the extent they will adopt "without-enrollment" scenarios. Some organizations standardize on it. Some allow it for companion devices such as a personal tablet. Others do not support it at all. Even in this last case, where an organization requires all employee devices to be enrolled in MDM, they typically support "without-enrollment" scenarios for contractors, vendors, and those with devices that have a specific exemption.

In Windows 10, one can even use Microsoft Intune's "without-enrollment" technology on enrolled devices. For example, a device enrolled in MDM may have "open-in" protections provided by the mobile operating system. Open-in protection is an iOS feature that restricts one from opening a document from one app, such as Outlook, into another app, such as Word, unless both apps are managed by the MDM provider. In addition, IT may apply the app protection policy to EMS-managed mobile apps to control the "save-as" feature or to provide multifactor authentication. Regardless of an organization's position on enrolled and unenrolled mobile devices and apps, Intune, as a part of EMS, has tools that will help increase workforce productivity while effectively protecting corporate data.

In macOS, MDM profiles for devices allow Apple's server applications to provision security policies, provide access to corporate accounts, manage certificates, and configure laptop settings. MDM profiles can also set passcode and encryption requirements, configure Wi-Fi and Ethernet adapters, manage native mail and Outlook accounts, configure network printers,

prevent software updates, and customize user experiences with dock and wallpaper settings. Profiles can be time-based and configured to deploy automatically or on demand. Apple scored lower in this area because the native server application that is purchased from Apple does not provide an out-of-the-box hybrid cloud solution. Apple also does not allow cloud providers to deploy macOS servers to manage large distributed enterprise solutions that have migrated to the cloud-based infrastructure or extended to a hybrid cloud solution.

Application Management

The following table summarizes the results of our hands-on testing of the application management capabilities provided by Microsoft and Apple. Microsoft outperformed Apple macOS in update management, mainly due to Apple's lack of controls for security and application updates. The scores of the two vendors were comparable in configurability and delivery, with iOS lagging a bit behind Windows 10 (and macOS) in configurability due to a more cumbersome and time-consuming configuration.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**36**	**35**
macOS High Sierra	**36**	**27**	**22**
iOS	**36**	**32**	**25**

The ability to whitelist or blacklist applications purchased from an app store for controlled images and licensing is important for any enterprise. Based on our testing, the Windows 10 white-/blacklisting functionality is a more granular and highly configurable solution in comparison to that of Apple and allows custom app and full app store selections. In contrast, macOS and iOS offer limited access to marketplace-restricted app stores when white-/blacklisting. By integrating with the Apple Volume Purchase Program (VPP) for managed app distribution, Apple MDM can upload and deploy commercial enterprise apps and LOB apps to macOS with defined app descriptions, images, and categories. Apple MDM can also distribute apps and remove apps if a user unenrolls his or her device. Commercial apps are available through the App Store, vetted, and digitally signed by Apple. Users cannot be restricted from installing personal apps from the App Store. Apps purchased with an Apple ID are available to other macOS devices configured with the same Apple ID. It is important to note that unless a separate Apple ID is provisioned, identity management will not be entirely functional.

Microsoft Intune provides device and application management and works seamlessly to deliver cross-EMS capabilities such as conditional access with Azure Active Directory Premium. Conditional access combines the power of Intune and Azure Active Directory Premium, allowing one to define policies that provide contextual controls at the user, location, device, and app levels. Natural prompts ensure that only verified users on compliant devices can access sensitive data.

Application configuration policies can help administrators eliminate these problems by allowing them to assign these settings to users in a policy before the users run the app. The settings are then supplied automatically, and users do not need to take any action. Intune can also be configured to assign applications to devices whether or not they are managed by Intune.

The following table outlines the various options for assigning apps to users and devices.

Application Whitelist and Management	Devices Enrolled with Intune	Devices Not Enrolled with Intune
Assign to users	Yes	Yes
Assign to devices	Yes	No
Assign wrapped apps	Yes	Yes
Assign apps as “Available”	Yes	Yes
Assign apps as “Required”	Yes	No
Uninstall apps	Yes	No
End users install apps from Company Portal app	Yes	No
End users install apps from web-based Company Portal	Yes	Yes

In comparison, the Apple Server console does not provide the administrators with many options for whitelisting applications, as the setting is Boolean in nature and access is either on or off. The administrator can select the types of applications and extensions, however, he or she needs to use the device section to define which applications can be used.

Remote Administration

The following table summarizes the results of our hands-on testing of the remote administration capabilities provided by Microsoft and Apple. Microsoft surpassed Apple in all four categories (asset management, OS/firmware update, security update, lost device) while Apple’s main relative weaknesses were the OS/firmware update and security update functionality for both iOS and macOS High Sierra.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**36**	**36**
macOS High Sierra	**36**	**20**	**17**
iOS	**36**	**34**	**29**

Being able to use remote administration from a central device management solution is very important, as this allows security professionals to perform investigations and helpdesk administrators to troubleshoot issues that a user may be experiencing. With the preceding mentioned deficiencies, scoring on this section was slightly one-sided in some ways, as macOS High Sierra was found to be lacking in its ability to push patches and use a peer-to-peer (P2P) style of update server offload. Windows 10, however, demonstrated a solid patch management approach with the ability to force patches and driver upgrades. In hands-on testing, the remote administration solution of Windows 10 overall performed much better than the remote administration of macOS High Sierra. In addition, being able to administrate a remote interactive session with a macOS desktop from the Windows 10 management suite using EMS and Microsoft Intune further increased the score for Windows 10.

EMS is not limited to pure mobility. Remote desktop functionality on the endpoint device is completely configurable and scalable in both on-premises and cloud solutions, including

hybrid deployments. Having the remote desktop function available to Windows 10 desktops, laptops, and tablets, including 2-in-1 solutions, has proven invaluable to the enterprise. Remote assistance with the desktop can be enabled via policy within Microsoft Intune.

Apple's MDM/Server 5.5 can query macOS devices for a similar variety of information, including hardware serial number, device name, and Wi-Fi MAC address. It can also query for software information, such as device version and restrictions, and list the apps installed on the device. When administrators need to update systems, application updates can be set to execute automatically, but the operating system needs manual user intervention that is never convenient for administrators. The overall management of an Apple solution is on-premises only. Apple does not support a cloud solution, as it lacks corporate cloud authentication mechanisms. Apple's narrow focus on identity management is limited to an iCloud account, which has limited scalability because it excludes the use of other federated authentication services.

Diagnostics and Monitoring

The following table summarizes the results of our hands-on testing of the diagnostics and monitoring capabilities provided by Microsoft and Apple. Windows 10 performed significantly better than macOS and iOS in the Anomalous Behavior Detection and Root Detection categories. Both Apple operating systems provide detailed crash reports; however, Windows 10 provides additional context around specific errors and reports, making it easier and faster for the administrator to respond.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**36**	**36**
macOS High Sierra	**36**	**18**	**17**
iOS	**36**	**18**	**17**

Scoring in this category leaned heavily on the Microsoft side of the score card, as the Windows 10 management suite offers full user behavior analytics capabilities, combined with application protection profiles and data leak prevention. In the case of Apple, we were unable to find this capability, as the server configuration was static in nature.

Apple can collect anonymous technical data used for improvement of products and services. This data is an opt-in process using the Diagnostic & Usage program to send nonidentifiable information about the device and applications. User-explicit consent is required to do this, and the user can view the data on the device or stop sending data at any time.

For Microsoft, EMS reporting is somewhat more extensive, as EMS can also report on abnormal and anomalous traffic for compliance as well as identify potential insider threats, data leakage, and intellectual property theft, in addition to generating the same types of reports produced by the Apple Server. EMS can also provide reports based on device status, user status, and application monitor logs including geographical reports. The level of detail that is available from EMS application protection reporting is extremely detailed and precise with no details left out.

Transparency and Granularity

The following table summarizes the results of our hands-on testing of transparency and granularity provided by Microsoft and Apple.

Testing Scores	Baseline	Feature	Functionality
Windows 10	**36**	**36**	**36**
macOS High Sierra	**36**	**26**	**12**
iOS	**36**	**27**	**11**

Windows 10 users maintain their own privacy settings under several device configuration policies. Many of the key management features regarding privacy are maintaining personal user privacy, as individuals have the right to access their personal data, correct errors in their personal data, and erase and export their personal data, as well as object to the processing of their personal data for purposes undisclosed. With a conditional enrollment policy for BYOD, users can have a certain amount of visibility into the settings maintained by enterprise policy, along with a limited capability in many cases to strengthen but never weaken the inherited policy enforced by the enterprise EMS.

Location awareness is equally covered by Microsoft and Apple, as both feature geo-fencing, essentially allowing access to enterprise resources of a specific nature based on the geographical locale of the user and device. Microsoft goes further with the ability to detect and alert on abnormal and anomalous user behavior. The data loss prevention and behavioral analytics capability further differentiates Microsoft from Apple in this category. Microsoft offers a comprehensive product suite that provides the administrator complete control over the entirety of the deployed infrastructure and endpoints. Microsoft Intune allows for full configurability of component management regarding the camera, the microphone, contacts, the calendar, and messaging parameters, while EMS controls and manages what data can be shared, in addition to features enhancing employee collaboration.

Compliance

The actions for noncompliance allow the administrator to configure a time-ordered sequence of actions that are applied to devices that do not meet the compliance policy criteria. By default, when a device is detected to be noncompliant, Microsoft Intune immediately marks it as such, and Azure AD Conditional Access blocks the device. The multiple options related to actions in case of noncompliance give the administrator more flexibility in his or her response—for example, deciding to not block the device immediately and giving the user a grace period to achieve compliance.

There are two types of actions:

- **Notify End Users via Email:** The administrator can customize the email notification before sending it to the end user. Intune provides customization of the recipients, subject, and message body, including company logo and contact information.
- **Mark Device as Noncompliant:** The administrator can determine a schedule in number of days after the device is marked not compliant. He or she can configure the

action to take effect immediately or give the user a grace period to be compliant with device compliance policies.

To make this work, the administrator will need to have created at least one device compliance policy for each platform. He or she will also have to configure Azure AD Conditional Access setup to use device compliance policies to block devices from using corporate resources, along with a template-created notification message. The notification message template is used later in the process of creating actions for noncompliance that are emailed to users. We did not find any evidence of cloud compliance or compliance reporting for Apple. For enterprise deployments, Apple will need to address these capabilities.

Patch Management

Microsoft Intune can help secure managed computers in many ways, including the management of software updates that keep computers up to date by ensuring the latest patches and updates are quickly installed.

When new updates are available from Microsoft Update, or a user created an update mechanism using a third-party tool, when the update is applicable to the managed computers, a notification is displayed on the Overview page of the Updates workspace. After an administrator or a user clicks this notification link, he or she can then perform various operations such as viewing more information about the update, approving or declining the update, and viewing the computers that will install the update if it is approved. One can also deploy updates for software not developed by Microsoft. This can be achieved by using the Upload Update wizard to get the update into the Cloud Storage space, after which one can approve or decline the update just like with Microsoft software.

In comparison, Apple does not publish a specific schedule for software or security updates. Instead, Apple periodically delivers version updates of macOS and iOS in addition to ad-hoc security fixes (such as the recent one for patching a macOS root password vulnerability) and other minor software updates. Apple macOS does not have a method for remote updates or separate security updates. It is recommended that the user keeps the default auto-update settings for Apple devices. That way, devices automatically update when the new release hits the Stable Channel. Unlike Windows 10 devices, Apple devices running macOS High Sierra or iOS cannot use P2P automatic updating. While this feature helps reduce external network traffic, Apple has not fully embraced this capability. With the P2P updating capability, EMS-enrolled devices automatically update from nearby devices, if they are the same model and if the organization’s network allows P2P connectivity. In addition, multicast DNS should not be filtered or blocked on the local area network. If P2P automatic updating fails or is not possible on the network, devices update through normal channels instead.

Conclusions

Based on an in-depth evaluation that included analysis of product documentation and hands-on testing, Pique Solutions concludes that Windows 10 provides a more comprehensive and easier-to-use management platform when compared to macOS and iOS. Besides the overall management functionality advantage of Windows 10 and EMS over Apple's management solution, we observed deeper management capabilities with Microsoft than with Apple in hybrid cloud scenarios, from device discovery over a hybrid cloud to application management. In all these scenarios, Windows 10 demonstrated to be an intuitive and scalable management platform, whereas macOS and iOS were limited to managing Apple-specific devices through Apple-managed servers. For macOS and iOS to provide the same management capabilities that Windows 10 with EMS offers natively, implementation and management of third-party MDM tools is necessary, along with the purchase of a server application add-on that runs as an additional service with various subcomponents. This increases the complexity and the total cost of managing devices and applications.

The recently accelerated pace of innovation and the new modern management capabilities introduced in EMS and Windows AutoPilot have allowed Microsoft to gain a substantial competitive advantage over Apple and further cement its leadership position in the enterprise. Pique Solutions found EMS to be a flexible, user-friendly, and scalable solution, with many features that are simple to navigate with support across multiple operating systems.

With EMS, Windows 10 can manage various devices, report on every facet of each device and user, deliver detailed behavior analytics, prevent data leakage, and maintain user privacy and identity protection. With Windows AutoPilot, provisioning and configuring a device is achieved extremely fast and with very little effort. These capabilities make Windows 10 a very powerful management solution, one that is better positioned than any other OS vendor, including Apple, to respond to the management challenges associated with digital transformation and increasing worker mobility demands, as well as growing privacy, security, and compliance requirements.

Among other key differentiators, we found that Windows 10 is better equipped to support remote enterprise administration. While most MDM solutions support enterprise domain authentication, Windows 10 leverages domain accounts as a single step for discovery, provisioning, configuration, and management of devices. Apple macOS requires a device to first be managed and configured through configuration files before business applications will support domain account authentication. Windows 10 also offers conditional access based on remote health attestation, something not yet seen in macOS, along with a much more comprehensive enterprise app management and update strategy.

Apple's management capabilities are suited for Apple devices and operating systems, with lack of support for the heterogeneous and complex device and operating system environments that exist in the enterprise today. In these complex environments, it is critical for organizations to be able to leverage management platforms with multi–operating system support. To be fair, macOS and iOS are flexible operating systems with several configuration options; however, we do not find them to be enterprise-ready platforms from a manageability perspective.