PIQUE SOLUTIONS

Device and Application Management

Windows 10 versus macOS and iOS

Manageability Feature and Functionality Comparison

PIQUE SOLUTIONS

MICROSOFT SPONSORED THE DEVELOPMENT OF THIS WHITE PAPER.

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

Executive Summary

With every enterprise operating system comes a methodology and means of managing workstations, servers, and mobile devices. While some operating systems require the use of third-party management tools to augment their functionality, others provide full functionality natively.

As organizations strive to align themselves with best practices of device and application management, they look for ways to accommodate the needs of both the business and the technical user with the objective of making them more productive. Often, this can be simply defined as "be patched and be functional with as little downtime as possible." While this sounds like an easy goal, managing across multiple operating systems and devices can become complicated.

While most OS vendors offer a management solution, their approaches vary. It is up to the enterprises to find a solution that accommodates their processes and management methods, while offering the highest security, functionality, and flexibility possible.

Moreover, many organizations today are moving parts of their IT infrastructure to the cloud to lower costs and increase productivity. This added complexity further changes the requirements for effective management, and the ability of the OS vendors to support these requirements becomes an important differentiator.

An effective management solution should offer the following capabilities:

- Multidevice management (MDM) capability.
- Multiplatform application management (MAM) capability.
- Self-service capabilities (i.e., password/PIN reset, installation of corporate-approved apps, and ability to join and manage groups).
- Ability to control access and protect corporate data.
- Support for a bring-your-own-device (BYOD) infrastructure and maintaining separation of ownership.
- Unified Endpoint Management (UEM), including desktop management.

Pique Solutions was commissioned by Microsoft to conduct a comparative analysis of the management capabilities of Windows 10 against those of Apple's macOS and iOS. The analysis will assess the level of assurance those capabilities provide an organization and the utility of those capabilities.

Microsoft offers a full suite of management tools that support on-premises, hybrid, and cloud environments. The key components of Microsoft's management suite are Intune, Systems Center Configuration Manager (SCCM), a part of Enterprise Mobility + Security (EMS), which is fully integrated with Office 365 and Windows 10 under the Microsoft 365 solution umbrella. These tools provide security and IT operations teams with granular, native controls over all devices within the enterprise, as well as devices that connect to the enterprise, regardless of the OS they run.

Like Microsoft's management suite, Apple's management tool—Apple Business Manager (ABM)—is free to enroll in but charges a fee to add devices. ABM provides management functionality to all Apple macOS and iOS device users. It also offers many features that are similar to those that Microsoft's EMS suite provides but with some important limitations, such as a lack of support for multi-OS environments and the need for implementing third-party tools to achieve several important management capabilities that Microsoft offers natively.

Study Approach

The methodology developed by Pique Solutions is as follows:

1. Determine the management characteristics and capabilities required to perform daily operations, as well as the ability to manage access to enterprise resources, including storage and sharing.
2. Evaluate through research how selected devices and operating systems used in conjunction with those devices are managed, and compare their relative strengths and limitations.
3. Publish a detailed assessment of findings.

To assess Microsoft Windows 10 and Apple macOS and iOS using industry-accepted standards and definitions, Pique Solutions referenced the manageability and required capabilities founded in the principles identified in Special Publication (SP) 1800-18 that cover privileged account management. Also referenced were industry best practices from the Data Interchange Standards Association (DISA), all correlated with various management techniques and capabilities as described by vendors. Keeping within the normal operating parameters of an enterprise-grade organization, based on practicality and functional management, enterprise management is not about being difficult or completely insecure but rather about balancing a functional enterprise operating system base while meeting enterprise goals.

To organize the presentation, we grouped the capabilities into the following three areas.

Device Management

- Device Enrollment: Ease of enrollment, controls, and compliance.
- Supported enrollment methodology, flexibility and functionality vs. strict.
- Management of multifactor authentication: Methods, store, use.
- Application management and restrictions.

Configuration and Policy

- Configuration Profiles: Roaming, geolocation, trust zones.
- Supported Encryption: Implementation of user and device roles for authentication and BYOD partitioning, software token storage, TPM support.
- Application Profiles: Group-specific allowed applications supported.

Administration

- Remote Administration: Application profile policy enforcement, OS policy and verification.
- Hardware Controls and Compliance: Hardware management, monitoring and reporting.
- Monitoring and Ownership: Services, application, usage.

For scoring, the criteria are defined based on Pique's subject matter expertise and, where appropriate, based on the preceding guidance of the NIST and DISA for management and configuration best practices.

We used the following scoring system (maximum score = 15).

Scoring Category	Score	Scoring Methodology
Feature	0 or 4	0 = Feature Not Present 4 = Feature Present
Native Functionality	0 to 3	0 = 3rd-party Tool Required to Achieve Full Functionality 3 = Full Functionality Native in OS
Granularity of Controls	1 to 3	1 = Low Granularity of Controls 3 = High Granularity of Controls
Functionality Compared to "Ideal Scenario"	1 to 5	1 = Low 5 = High

This white paper compares Windows 10 version 1809 to Apple macOS 10.14.3 and iOS 12.1.

Device Management

Device management has become a mainstay in everyday IT operations. As more companies introduce mobile platforms to enhance workforce productivity, the network perimeter has become something that users hold in their hands. Mobile devices available today allow access to every part of the enterprise infrastructure and enable employees to work from anywhere.

Policy management is one of the most efficient methods to control access to data, but only after exploring multiple solutions and what they offer in terms of compliance, policy enforcement, and flexibility can we determine the best device and application management solution for the enterprise.

The most common form of device management in a Windows 10 environment is called Group Policy, which is issued at the time of log-in. This is also the most antiquated method of device management with serious limitations. Over the past several years, Microsoft has made many advancements in this area as it recognizes the need to manage devices with various operating systems in one environment.

Apple not only shares a vision similar to that of Microsoft in terms of device management but has also provided an intuitive user interface with a complete suite of MDM tools, enrollment options, and content management configurations. While this visually pleasing interface is easy to use, it fails to address some key management issues, such as antivirus, risk-based security policies and support for user and entity behavioral analytics. In addition, the limitation of not being able to support anything other than Apple devices and operating systems leaves a large gap in the ABM platform.

ABM has been able to provide granular security and application and network management configuration controls that comply with NIST and Department of Defense (DoD) standards, while also being able to define multiple Device Enrollment Program services that can each have separate policy mandates, similar to those of User Groups within Microsoft's EMS platform. Apple has also achieved multitenancy within an organizational environment. True multitenancy in a single org is something that Microsoft has yet to provide, short of creating multiple active directory forests.

Windows 10 also successfully integrates with multiple authentication methods and standards, making it a robust operating system that can be easily deployed to most IT environments and effectively managed. It has yet to provide a true organizational multitenant environment without co-mingling data.

The migration of traditional PC management to UEM tools is a key step in transforming to modern management. Microsoft's UEM solution, Intune, has seen continual improvement in features and overall functionality for managing not just Windows 10 tablets and phones but all mobile devices and desktops, regardless of the operating system on which they run. This makes Microsoft Windows 10 the most flexible operating platform. Through Intune's console, IT administrators can execute a UEM strategy where end users can be onboarded through any hardware platform, and rules can be applied governing which applications and what data they can access. UEM uses MDM APIs on mobile platforms to enable identity management, wireless LAND management, operational analytics, and asset management. UEM enables IT to remotely provision, control, and secure everything from smart phones to tablets, laptops, desktops, and Internet of Things devices from a single management console. Combining the capabilities of Intune and SCCM enables users to manage Windows PCs and servers, Macs, and Linux/Unix servers, as well as mobile devices running Windows, iOS, and Android—all through a single administrative console.

This is an important differentiator for Microsoft, as Apple does not provide UEM capabilities natively but instead requires integration of third-party UEM tools, which adds complexity and increases costs. In

addition, Apple's ABM MDM solution provides limited functionality, as it can only manage registered iOS and macOS devices.

ABM also provides limited functionality in that it can only manage iOS and registered Apple macOS devices. Apple fails to provide its own UEM solution and requires integration with a third-party UEM provider like MobileIron to perform UEM functions at an additional $6 per device per month subscription. Once integrated with third-party UEM tools, Apple's platform is flexible but also costly.

The fact that Windows has become the standard operating system for most enterprises motivates Microsoft to continue producing a best-of-breed management solution that can scale while also maintaining security, compliance, and policy enforcement.

Apple has become a market leader in the artistic design industry over the years and has become favored in the start-up company space in terms of popularity in sales and marketing departments. IT operations have had to work harder in the past as IT administrators integrate macOS systems into corporate Active Directory systems and third-party patching systems. ABM has made the integration easier from a hybrid cloud perspective. **Table 1** provides a summary of scoring for Device Management features and functionality.

Table 1. Summary of Scoring Results for Device Management

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	●
macOS	◑	◕	●	◕
iOS	◕	◕	◕	◕

Poor ○ ◔ ◑ ◕ ● *Excellent*

Mobile Policy

Being able to define a policy to protect enterprise devices, regardless of the operating system, is one key foundation of being able to enforce policies such as geographical resource restrictions, remote device wiping, data restrictions based on risk, and multifactor authentication.

While it's not always practical to restrict every part of a mobile device, as it limits its overall usability, in many cases a restricted device will save an enterprise from falling victim to malware or a botnet.

The most common policies are BYOD and corporate-owned device (COD). Enterprises rely on both BYOD and COD when they do not have the budgets to support a COD policy alone or they allow employees to use their own devices and subsidize the monthly fees to compensate for restrictions placed on personal property to protect the enterprise.

Not only can Microsoft Intune manage device policies across all Windows 10 devices, as well as Android 9 (Pie) and Apple macOS and iOS devices, but the platform also offers many options for policy enforcement with many moving parts around device enrollment, user authentication to restricted data,

and geolocation risk policies. This creates a complex and somewhat complicated user experience at both the interactive and API levels.

Apple has maintained a simple and easy-to-navigate admin console experience with a software development kit that allows administrators with little to no coding experience to develop applications for the enterprise, easing the facilitation of management tasks.

Microsoft's new software APIs for EMS still prove slightly cumbersome and require intermediate programing skills to effectively create additional applications to enhance the management experience.

Application Policy Restrictions and Profiles

Application policy is more than just determining the limits of the user's ability to side-load unauthorized applications. It allows IT operations teams to set restrictions on circumstances that would put the enterprise at risk, based on user type (e.g., executive, privileged admin user, contractor), geographical location, user behavior, or a combination of all three.

Microsoft EMS enables IT operations and security teams to define multiple policies based on location, behavior, and general authorized application policies, allowing enterprises to create more dynamic policies that can be activated based on user risk, geolocation, and user types. With Intune and SCCM, users can self-provision applications through a company portal and check for compliance. They can install and run corporate applications across devices from a single management console.

Apple has made similar advancements in this space but is still relying on third-party UEM providers to offer a complete solution using Apple's integrated framework.

Intune provides device and application management and works seamlessly to deliver cross-EMS capabilities such as conditional access with Azure Active Directory (AD) Premium. Conditional access leverages the power of Intune and Azure AD Premium together by allowing one to define policies that provide contextual controls at the user, location, device, and app levels. Natural prompts ensure that only authorized users on compliant devices can access sensitive data while providing self-service requesting access to applications and data using built-in forms and click-throughs. This flexible and scalable management solution allows enterprises to maintain a leaner IT operations team. A self-servicing management environment allows the end-user to make requests to enterprise data and applications, providing an auditable solution that holds data owners accountable for access and puts less demand on IT operations.

Remote Administration

Remote desktop and device administration has seen an increase in the use of third-party products that offer secure multifactor administration, with recordings of user interactions, password management for privileged accounts, and a combination of both depending on the sensitivity of the system. Many of these third-party applications offer secondary logging options for authentication mechanisms to enhance and validate the system-based logging.

Being able to use remote administration from a central device management solution is very important, as this allows security professionals to perform security investigations and helpdesk administrators to troubleshoot issues that a user may be experiencing. Both macOS and Windows 10 offer a solid remote administration solution. Where Windows 10 remote administration really makes a difference is with its remote administration of Android devices. The ability to have a remote interactive session on an

Android phone or tablet from the Windows 10 management suite illustrates the flexibility of the Windows 10 operating system. Using Intune, EMS can set policy to allow remote administration.

Remote desktop functionality on the endpoint device is completely configurable and scalable in both on-premise and cloud solutions, including hybrid deployments. Having the remote desktop function available to Windows 10 desktops, laptops, and tablets, including various PC manufacturers' 2-in-1 systems, has proven invaluable to the enterprise. Remote assistance and remote desktop can be enabled via policy within Intune. Using the TeamViewer service within UEM, administrators can remotely access iOS and macOS devices. Windows 10 administrators can also remotely manage macOS devices within the enterprise.

This is not to be confused with Remote Desktop Protocol or any local remote desktop application, as it's regarding the manageability of the operating system using an agent or API via the management console of each respective management platform.

The closest solution that natively fits into the ideal scenario in this case is Microsoft's EMS suite tied in to Azure and Office 365 services.

Configuration and Policy

While many organizations see configuration and policy as a compliance and governance issue, they are also closely tied to security and asset management. For compliance management to be truly effective, identifying the business and technical owners who manage and maintain each program (e.g., the network, email, device management) is imperative to the success of policy enforcement and device configuration.

Both the business and technical owners' requirements for successful outcomes are guidelines for the configuration and policy as it complies with security and organizational privacy restrictions. Internet technology system management (ITSM) platforms provide additional clarity when paired with compliance, vulnerability, and operating system management. Using vendor-provided management solutions with an ITSM can remove the risk of untested changes, inaccurate archives, and unforeseen consequences. **Table 2** provides a summary of scoring for Configuration and Policy features and functionality.

Table 2. Summary of Scoring Results for Configuration and Policy

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	●
macOS	◑	◑	●	◑
iOS	◕	◑	◕	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*

Profiles

As a best practice, configuration profiles are traditionally administered at an organizational and group level, because individual configuration profiles are neither scalable nor manageable. Microsoft supports this model by providing a flexible solution that accommodates the various role-based access and discretionary models of authentication and authorization.

ABM fully embraces role-based access, as its profile configuration is focused on the enterprise. but it still relies on a third-party solution to satisfy many of the UEM requirements of most enterprises. Group policy is also taken into consideration, and it conforms to industry best practices regarding NIST and DoD standards.

Encryption

Choosing the right encryption solution can be difficult with a myriad of unseen pitfalls that do not often present themselves until after deployment. What most organizations don't realize is that most operating systems offer some form of built-in device encryption. Vendor-supported encryption methods are mostly found to be supported in the management platform for the operating system, with dynamic key management and rotation policies available. Many security administrators argue that third-party encryption solutions are the only way to secure desktops and mobile devices, as they are always running optimized encryption algorithms of the highest standard. The fact of the matter is that the natively supported encryption methods and tools, which are optimized for the operating system, are a more effective approach to management.

Encryption is the primary means used to ensure a lost, stolen, or misused device does not lead to the loss or compromise of sensitive information. The cryptographic keys used for encryption should be stored in protected locations in software, firmware, or hardware, with hardware providing the highest level of protection. Tamper-resistant hardware is also preferred for performing cryptographic operations.

Windows 10 management allows a multitude of authentication mechanisms that are commonly used within the enterprise today. This approach from Microsoft enables enterprises to use a single platform to manage users, data access, and devices.

Windows 10 Enterprise allows multiple authentication methods to be deployed, taking advantage of smartcard technology and biometrics. Windows 10 allows for both traditional fingerprint and facial recognition, enabling the enterprise to maintain a strict security posture.

Apple has fully integrated biometrics into the macOS and iOS platforms. Depending on the type of Apple device, however, the biometric method may vary. While MacBook Pro, iPhone 8, and iPad offer traditional fingerprint biometrics, the newer iPhone X and iPad Pro only offer facial recognition. The inconsistency in biometric methods from Apple leaves enterprises with security and management gaps, as biometrics are not available in either iMac or MacBook products.

Application Profiles

Managing application profiles can limit abuse and fraud waste management. Administrators taking advantage of application profiles can effectively manage application licenses and lower the security risks at a group level within an organization by limiting application security exposures.

Both Microsoft and Apple provide administrators with the ability to create application profiles that contain a list of both acceptable and unwanted applications. Microsoft's UEM lends itself to AI and machine learning, as all behavior is modeled, analyzed, and retained for future events. Apple can only achieve the same level of functionality when combined with a third-party platform. Microsoft also learns geographical and user actions provided all logging is enabled.

As Microsoft has been building user access models for quite some time, they provide a richer management environment that looks at many of the possible scenarios and enables system and security operations teams to take advantage of every possible configuration setting.

Using the Microsoft application profiler and insight products, administrators can quickly define the parameters of what version of the application will be made available to the end user along with in what region and under what circumstances a user can use an application.

Like Microsoft, Apple has also achieved this level of control in the enterprise space, offering customizable application stores depending on the types of restrictions imposed on an organization.

Microsoft is clearly making the most advancements in this area of Windows 10 device management, with an agnostic approach toward flexible application profiles available across multiple device and OS types.

BYOD Enrollment and Quarantine Policy Management

Recognizing that employees often work best when they're allowed to choose their own tools, BYOD policies let people use their own devices, whether occasionally, primarily, or exclusively, for work.

One of the most obvious challenges is how people are going to be able to access enterprise applications and corporate data and files on their personal devices. Simply installing apps directly on the device would raise serious security, privacy, and compliance risks, license management issues, and support complications, as well as restrict employees' choices to Windows-based devices.

Ideally, a flexible management frame lends itself to a BYOD model and either a choose-your-own device, a COD, or a personally enabled device. A combination of all three strategies allows for greater flexibility and can lower abuse from a fraud and waste management perspective. Other capabilities that should be taken into consideration are as follows:

- Management of multiple device types.
- Partitioning of corporate and personal data.
- Enablement of self-service provisioning of services.
- Mobile device quarantine capability.
- Policy enforcement.

Device quarantining allows organizations to limit their exposure to high-risk individuals who are traveling to unfriendly environments that are known for corporate espionage and stealing of intellectual property. Quarantining also limits malicious software and noncompliance with corporate policy.

Microsoft offers several methods and tools for device enrollment. Users can 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 will be reconfigured with the settings approved and enforced by IT. Some 400 common settings are available to the administrators 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 so on.

Other methods of enrollment include conditional access. This method is ideal for BYOD solutions where employees and contractors can use personal devices for business with granular restrictions that will occur when the employee or contractor leaves the organization. Email will be wiped along with all contacts owned by the company, in addition to any associated apps installed by the company along with content and settings.

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 platforms.

In addition, using Windows AutoPilot, a user can take delivery of his or her 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 for enterprises adopting the modern management principles empowered by the cloud. For those organizations that are yet to make that transition, Microsoft has tools and processes in place to assist customers who currently do not utilize any cloud services but are interested in a shift to modern management. For example, a co-management method using Intune and SCCM lets users attach their existing SCCM deployment to the Microsoft 365 cloud. It helps users unlock additional cloud-powered capabilities like conditional access.

ABM uses Apple ID for identity management. Enrolling devices into the device manager is more time-consuming and cumbersome in comparison to the enrollment process of Windows 10 and Microsoft EMS. After the initial enrollment into ABM, any devices purchased outside of Apple need to be purchased through an approved partner at an undisclosed fee and the Reseller ID 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.

Cloud Management

Perimeter system management does not have a common topology in today's enterprise landscape. Enterprises are becoming more agile, lean, and mobile. Being able to keep up with the demand of a modern enterprise from an on-premises architecture means personnel will always be required in the office or datacenter. Today's solutions need to be flexible and allow administrators to take advantage of lower-cost infrastructure and improve the overall user experience. Using cloud-based vendor services that enable the system administrators to enforce policy across multiple device types with the click of a button becomes a priceless feature.

To reduce the impact of misconfiguration and external exposure, vendors can help place account restrictions on access to cloud services and provide device administrator profiles to accommodate organizational policies and corporate standards.

Cloud management has traditionally lent itself to a managed security service provider model. Today, cloud providers are offering cost-effective pure cloud and hybrid solutions that let enterprises maintain critical assets within their well-protected perimeter, while moving other services such as directory

services, mail, and application and mobile device management to the cloud, often retaining the ability to fall back onto the on-premises solutions if necessary.

Microsoft has been able to build a complete cloud-based infrastructure that incorporates directory services, policy, device, and mobility management in a single entity. **Table 3** provides a summary of scoring for Cloud Management features and functionality.

Table 3. Summary of Scoring Results for Cloud Management

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10				
macOS				
iOS				

Poor  *Excellent*

Compliance and ITMS Governance

Device management is not just about adherence to corporate policies and security. It's also about being able to audit for compliance checks and, in many cases, about asset management. Assessing the additional risks from BYOD and allowing for personal enablement of corporate devices pose several risks and can open up a company to many new issues it had not considered before the rise of BYOD.

The actions for noncompliance allow administrators to configure a time-ordered sequence of actions that are applied to devices that do not meet compliance policy criteria. By default, when a device is detected to not meet these criteria, Intune immediately marks it as noncompliant, and then Azure AD Conditional Access blocks the device. The actions for noncompliance give administrators more flexibility when deciding what to do when a device is not compliant. For example, they can decide to not block the device immediately and give the user a grace period to become compliant.

The two types of actions are the following:

- **Notify End Users via Email:** Customize an email notification before sending it to the end-user. Intune provides customization for the recipients, subject line, and message body, including company logo and contact information.
- **Mark Device Noncompliant:** Determine a schedule in number of days after the device is marked not compliant, and then configure the action to take effect immediately or give the user a grace period to become compliant with device compliance policies.

To make this work, the administrator needs to create at least one device compliance policy to set up actions for noncompliance and then create a device compliance policy for each platform. Azure AD conditional access should be set up when planning to use device compliance policies to block devices from using corporate resources. A notification message template is also created, which is later used when determining actions for noncompliance to send to users via email.

ABM is designed specifically with strict privacy and security standards based on industry-wide best practices. For organizations with compliance standards, the ABM portal is fully adherent. With device and user compliance standards enforcement, the ABM portal makes for a hard security target.

Initially, Apple offered a very limited set of security management features for IT administrators from within the ABM portal, after realizing the shortcomings of the configuration, enforcement, and the lack UEM support. Apple reacted with a flexible framework to work with existing technology and to partner with market leaders to provide rich third-party solutions. Enterprises should carefully examine Apple's required level of third-party access needed to successfully deploy ABM.

Apple released ABM less than a year ago and already it has demonstrated that, with the integration of third-party platforms, users can take full advantage of a scalable UEM solution without needing to leave the ABM user interface.

Windows 10 administrators have full control to review and establish security policies around sharing content and inviting external users across various applications. This allows administrators to create customized policy infrastructures to meet the unique security demands of their organizations.

Conclusions

As businesses look for ways to provide employees with flexible work environments that bolster productivity, whether on desktops or mobile devices, in the office or out in the field, IT organizations are expected to consolidate the management of desktop and mobile devices of disparate operating systems into a single management console. This trend has facilitated the advancements and adoption of UEM solutions, which allow all user-facing devices to be managed from a single console.

Microsoft and Apple have taken different approaches to addressing these needs, and these differences have important implications on users. While Microsoft offers full functionality required for modern device and application management natively with Intune, Systems Center Configuration Manager, and Microsoft EMS, Apple customers are required to procure, integrate, and manage third-party tools to achieve the same functionality and granularity of management controls.

In addition, while Microsoft Intune is tied to Windows 10 and other Microsoft products, it is designed to manage hardware running other operating systems. In contrast, ABM natively only manages iOS and macOS devices. Again, third-party MDM/MAM tools are needed for managing environments with multiple operating systems.

The need for Apple customers to deploy third-party tools to achieve these important management capabilities increases the complexity of management and puts Apple at a disadvantage versus Microsoft with respect to both ongoing operational costs and user productivity.

Other key differentiators are Microsoft's use of behavioral analytics combined with risk and geography-based access policies across multiple operating systems and devices, whereas Apple's limited reach fails to address management needs in environments where multiple device types and operating systems coexist. It is Microsoft's OS- and device-agnostic approach that sets it apart from other vendors providing a comprehensive, scalable management solution for enterprises of all sizes and IT environments.

As **Table 4** shows, throughout our assessment, Windows 10 demonstrated superior features, native functionality, and granularity of controls than both macOS and iOS.

Table 4. Summary of Cumulative Scoring Results for All Categories

OS	Feature	Native Functionality	Granularity of Controls	Functionality vs. "Ideal"
Windows 10	●	●	●	◔
macOS	◑	◑	◕	◑
iOS	◕	◑	◕	◑

Poor ○ ◔ ◑ ◕ ● *Excellent*