jamf

UEM

WHY

UNIFIED ENDPOINT MANAGEMENT

UEM

FALLS SHORT

And how to overcome its flaws

Remote or hybrid workforces are here, and users are using more and more devices to stay connected and productive.

Organizations need to manage, support and secure the range of end-user devices, but may be asking,

“How do we manage the various platforms in our environment?”

Because organizations and their users have devices across different operating systems — and with employee-choice programs, this challenge will only be more prevalent in the modern workforce — different operating systems and devices deserve dedicated solutions.

The notion of unified endpoint management (UEM), where all devices are managed with a single mobile device management (MDM) solution might sound great, but begs the question,

“What is universal across Microsoft, Apple and Google?”

The reality is desktop operating systems — Windows, macOS and Chrome OS — have little in common.

Each have a unique workflow to provision, encrypt, deploy, secure, update and support devices. The same distinctions apply to the mobile platforms: iOS/iPadOS, Windows Mobile and Android.

UEM falls short; no one management tool is designed to support everything.

So, your organization has likely considered:

- **Managing devices by platform type**

  (i.e., desktop or mobile)

- **Attempting to manage your devices with a unified tool.**

- **Managing your devices by ecosystem**

  (Apple, Microsoft, Google)

This e-book breaks down your choices and their impacts on your organization and end users to help you determine the right management philosophy and solution.

APPROACHING MANAGEMENT THROUGH THE LENS OF AN ECOSYSTEM

Defining device management models

Let's start by examining the various types of device management models.

Whether you manage your devices separately by device type or attempt to put them all in one unified tool, you are forced to support the lowest common denominator. The lack of commonalities across various device types coupled with unique and frequent upgrade cycles, means there is no one-size-fits-all approach to device management.

> The reality is that unified management tools aren't designed to support every device type and platform, and organizations are often relegated to a "master of none" toolset.

OPTION 1

Devices Managed by Type

Rather than focusing on the individual devices you manage, what happens when you focus on the ecosystems (i.e., platform or brand) you manage? When you organize vertically by ecosystem, commonalities arise.

Device Type	Apple	Microsoft	Google	Management
✖ Computer	macOS	Windows	Chrome OS	Client Management
Mobile	iOS/iPadOS	Windows Mobile	Android	EMM/MDM Tool
TV	tvOS	—	Chrome OS	EMM/MDM Tool

OPTION 2

Devices Managed by a Single Tool

Windows and Windows Mobile have commonalities, and Microsoft provides first-party management tools with Microsoft Endpoint Manager and System Center Configuration Manager (SCCM). Chrome OS and Android are moving closer together, and both can be managed by Google's native management tools in G Suite. And, because Apple is known for creating an integrated IT and user experience across all of its device types, it best illustrates the value of managing devices by ecosystem.

✖

Device Type	Apple	Microsoft	Google	Management
Computer	macOS	Windows	Chrome OS	UEM
Mobile	iOS/iPadOS	Windows Mobile	Android	UEM
TV	tvOS	—	Chrome OS	UEM

OPTION 3

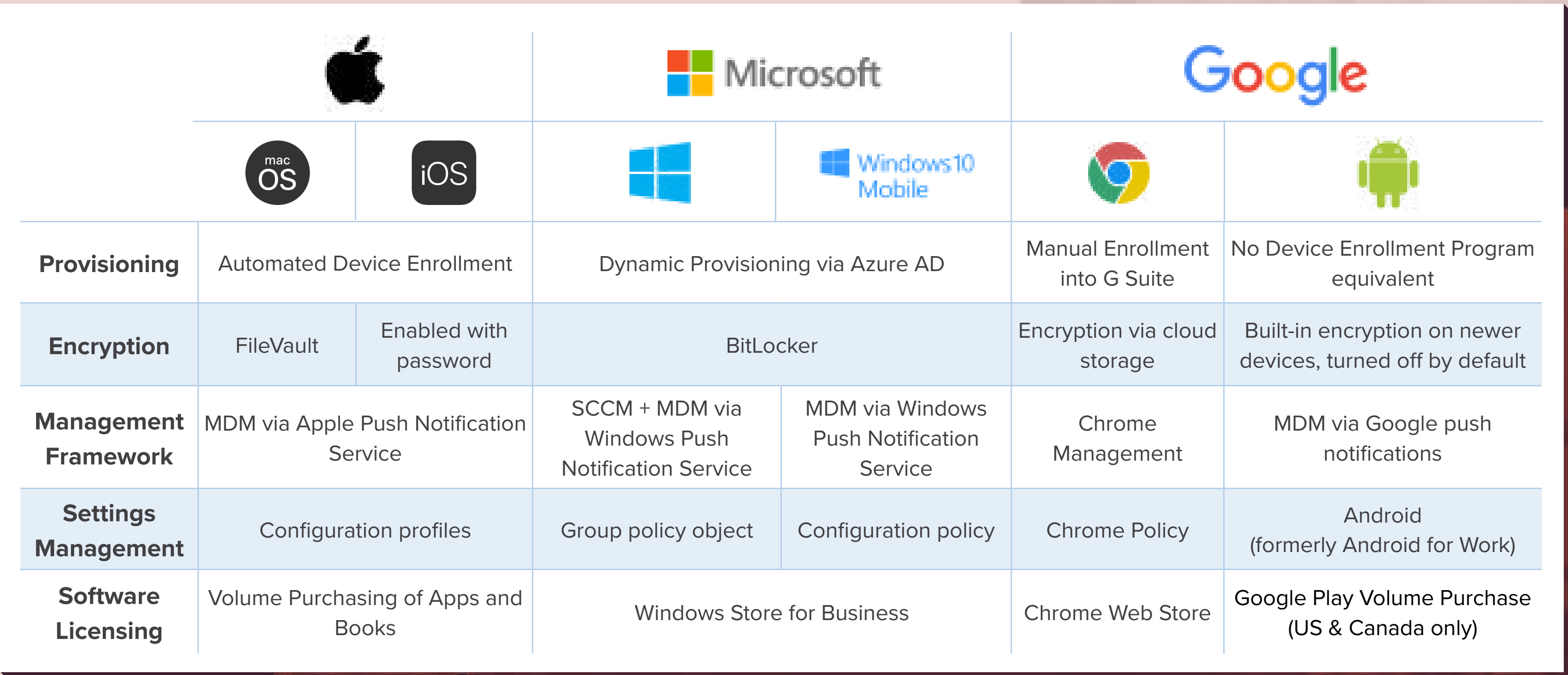
Devices Managed by Ecosystem

Apple operating systems converge, and by design, function as an ecosystem. To get the most out of the Apple ecosystem, iOS, iPadOS, macOS and tvOS devices should be managed together with a purpose-built management solutions, such as Jamf.

Device Type	Apple ✓	Microsoft	Google
Computer	macOS	Windows	Chrome OS
Mobile	iOS/iPadOS	Windows Mobile	Android
TV	tvOS	—	Chrome OS
Management Tool	**Jamf**	**Intune/SCCM**	**G Suite Management**

Efficiency gains for IT

By choosing to manage devices by ecosystem rather than device type or unified tool, management tasks are optimized without compromising native functionality. Let's explore the different ecosystem workflows for Apple, Microsoft and Google.



			Microsoft		Google	
	mac OS	iOS		Windows10 Mobile		
Provisioning	Automated Device Enrollment		Dynamic Provisioning via Azure AD		Manual Enrollment into G Suite	No Device Enrollment Program equivalent
Encryption	FileVault	Enabled with password	BitLocker		Encryption via cloud storage	Built-in encryption on newer devices, turned off by default
Management Framework	MDM via Apple Push Notification Service		SCCM + MDM via Windows Push Notification Service	MDM via Windows Push Notification Service	Chrome Management	MDM via Google push notifications
Settings Management	Configuration profiles		Group policy object	Configuration policy	Chrome Policy	Android (formerly Android for Work)
Software Licensing	Volume Purchasing of Apps and Books		Windows Store for Business		Chrome Web Store	Google Play Volume Purchase (US & Canada only)

As you can see, the different ecosystem workflows require different ways to provision devices, apply settings and deploy software. And, this lack of universal workflows alone should be argument enough that unified endpoint management is not the correct method to manage multiple ecosystems.

However, if you manage your enterprise fleet by ecosystem, you can achieve the best of both worlds — efficient management and security for your IT team balanced with productive and happy end users.

Let's look at how Apple's ecosystem shares management commonalities across **iOS**, **iPadOS**, **macOS** and **tvOS**.

WHY APPLE FIRST: THE INTERCONNECTED EXPERIENCE

Apple continues to build an interconnected ecosystem.

In fact, they are the leading example of a cohesive desktop and mobile experience. Apple embraces a consistent user experience across their entire ecosystem. iMessage, FaceTime and other continuity features work across all Apple devices. For example, users can unlock their Mac from their Apple Watch, create a presentation on their Mac, continue editing the presentation on their iPad and then present via Apple TV.

The cohesive Apple ecosystem creates the incredible experience users expect, and caters to IT in an enterprise setting. Apple has specific enterprise programs to help streamline deployment and create an out-of-box experience for users. Automated Device Enrollment and Volume Purchasing of Apps and Books, combined with a mobile device management (MDM) solution, ensure consistent management of iPhone, iPad, Mac and Apple TV.

Apple's native management functionality in **Apple Business Manager/Apple School Manager** paired with an ecosystem-specific MDM allows IT to deploy, manage and secure Apple devices.

Keeping pace with ongoing updates

Ensuring a seamless experience for your users is an ongoing process — one that includes continually supporting new features and capabilities on your devices. Apple, like other technology providers, have regular upgrade cycles for their operating systems, so it is critical from both a security and functionality standpoint to ensure your users can upgrade to the latest releases.

With every new release, iOS/iPadOS, macOS and tvOS become more integrated with each other, and Apple users are quick to upgrade to the latest features.

WHY?

The upgrade process is simple, free and they want to take advantage of the latest capabilities.

While new operating systems and features enhance the user experience, users only benefit from the latest and greatest if and when all of their Apple devices are fully supported. And often, IT and security teams want or need to control an end user's ability to upgrade and update until security patches or fixes can be made at the organization-wide level. Supporting your fleet with an ecosystem method and tool allows you to control the release cycle and support updates across all devices to greater effect and with greater speed.

When organizations subscribe to the UEM model, they're reliant on a vendor's ability to support multiple and competing maintenance cycles which, because of the lofty task of supporting distinct and complex systems, often results in resource and time constraints, not to mention a result that caters to the lowest common denominator.

As a result, updates to the latest platform are often delayed by months, quarters, or worse, never supported.

Beyond diminishing the user experience, when UEM software can't immediately adopt the latest platform updates, organizations using those tools are exposed to security vulnerabilities and broken workflows. The best way to keep users productive and your organization protected is through a purpose-built solution that immediately supports updates to each platform's specific ecosystem.

This isn't a luxury, but rather a baseline requirement for successfully securing and protecting your devices.

Software licensing and app purchasing under one roof

Apple's ecosystem of apps sets them apart from others on the market. Apps are core to enabling user productivity, and Apple has a rich App Store. However, downloading apps from the App Store traditionally required an Apple ID.

Volume Purchasing of Apps and Books is a streamlined method for purchasing and managing apps in bulk, and it's the only method to distribute App Store apps to your managed devices. Leveraging a single ecosystem management solution streamlines deployment and management of these apps. Furthermore, keeping purchasing, assignment and distribution all linked to a single ecosystem management solution reduces complexity and avoids potential loss of data.

Volume Purchasing of Apps and Books with an Apple management solution supports an organization's ability to:

Purchase

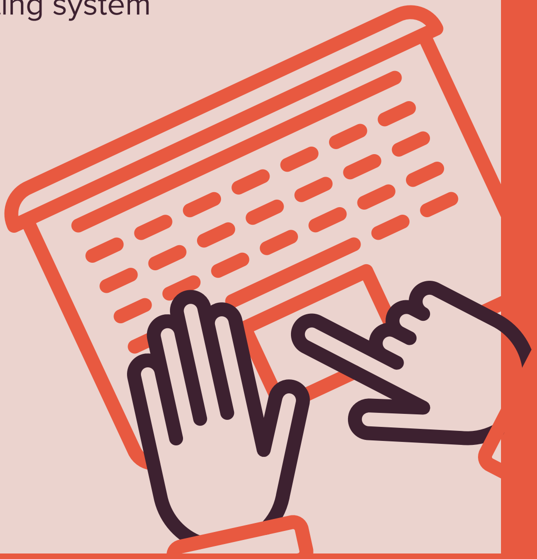
IT purchases all Apple apps in one central location regardless of the device / operating system

Assign

App assignments are easier with a single volume purchasing account because all available purchases are linked to one central location versus accounts. Apple IDs are not required for device-based assignments

Distribute

Volume Purchased Apps and Books are all listed in your single MDM and ready to be deployed to users



User resources under one roof

Users demand the same seamless technology, support and service experience regardless of what device they use, and this expectation doesn't stop once the device is in their hands.

There are many ways to extend the consumer Apple ecosystem experience. One way to do so is through a management app.

A management app enables IT to curate assets and provide users with an easy way to obtain resources and services, such as apps, printers, troubleshooting shortcuts and documentation. Anything loaded in the app is IT-approved, so instead of submitting a ticket, employees go directly to the app and immediately download the needed items — saving time for both you and your users.

Segmenting your Apple devices in separate management solutions forces end users to interact with different apps for Mac and iOS, ultimately creating confusion for where to go for what device. Streamlining ecosystem management with one solution gives you a common app for all Apple platforms. Users gain a consistent experience with a portal that has one brand, name, look and feel across iOS, iPadOS, macOS and tvOS.

What about Apple IDs?

Apps can leverage iCloud to sync mobile, desktop and even Apple TV operating systems. This allows the user to start utilizing an app on their iPhone and then pick up right where they left off on their Mac. App hand-off and sync is possible because of a user's Apple ID. If your information security team approves of iCloud, you can allow your users to use their own Apple IDs and still deploy apps via device-based assignments.

WHERE ECOSYSTEMS INTERSECT

Reporting tools as your single pane of glass

The need for a holistic view into your environment is undeniable. Commonly referred to as a single pane of glass, you want the status of all endpoints, the ability to generate reports for senior management, and have a 360-degree view into your inventory. While UEM providers pitch this as the core reason for one universal tool, the lack of up-to-date support for the latest platform features overshadows the value of what you get with one window into your world.

Instead, look to proven, purpose-built business intelligence and reporting tools for your single pane of glass. Rather than reporting from your device management tool alone, aggregate the data into a BI or IT service management tool (e.g., **Domo**, **Splunk**, **Tableau** and **ServiceNow**), which is designed to show dashboard data. This lets each ecosystem management tool do what its designed to do best — connect, manage and secure devices and users. All device data can then be sent to a reporting / BI tool.

Devices Managed by Ecosystem

	✓		
Device Type	**Apple**	**Microsoft**	**Google**
Desktop	macOS	Windows	Chrome OS
Mobile	iOS/iPadOS	Windows Mobile	Android
TV	tvOS	—	Chrome OS
Management Tool	**Jamf**	**Intune/SCCM**	**G Suite Management**
Reporting Tool	**BI Tool: ServiceNow. Splunk, Tableau, etc.**		

The power of "and"

When managing an ecosystem, it's important to consider a management solution that fits seamlessly into your existing IT infrastructure.

Services such as identity access management, directory services and network access, which may already be in your environment, are becoming platform agnostic and should extend across your managed ecosystems. Identity management, network access control and directory services can easily work with **Apple**, **Microsoft** and **Google** devices, but are not directly built into most device management solutions.

Instead, with Apple, organizations and enterprises can rely on purpose-built solutions to handle identity management, directory services and network access to do what they do best rather than hoping a unified tool can do it all. An integration-friendly ecosystem device management tool that can connect to existing IT services is better for organizations in the long run because it leverages what's best about the platforms while fitting into a broader IT strategy.

Jamf Integrations

The Jamf platform is able to integrate with third-party tools, such as **ServiceNow**, **RobotCloud**, **Tableau**, **Splunk**, **SCCM** and **Microsoft Endpoint Manager** to share your Apple inventory data. This provides better reporting and better management for your Apple devices.

Embrace Apple Enterprise Management

When organizations apply solutions that were designed for non-Apple operating systems, they fall short and often leave IT and users vulnerable to security threats, high-cost breaches or simply poor experiences and inefficiencies.

Apple Enterprise Management fills the gap between what Apple offers and the enterprise requires, and provides IT with an unmatched and complete toolset to fully empower users.

With Jamf, enterprise management starts at device deployment and supports users and organizations to the end of the life cycle.

Deploy

With zero-touch deployment, you're able to deploy devices to any employee, anywhere. Getting started is easy, accessible and the experience end users expect from Apple.

Manage

Remote management for devices, inventory and apps is just the start. With hundreds of integrations and partnerships with Microsoft, Google, and many more, the power to manage your enterprise needs goes well beyond simple MDM solutions.

Connect

Identity-based access and Jamf's Self Service app empowers users from the point of onboarding through ongoing support with secure and easy access to your network and resources.

Protect

To ensure the success and safety of Apple in the enterprise, organizations need Apple-specific security solution preparing for, preventing and detecting threats, and remediating security incidents.

SELECT THE RIGHT SOLUTION FOR YOUR ECOSYSTEM

Microsoft, **Google** and **Apple** provide unique experience across each of their desktop and mobile platforms and require dedicated management solutions.

Jamf is the tool trusted by those who trust Apple.

If you're ready to move beyond the failed vision of UEM and see the benefits of Apple Enterprise Management for yourself, request a free trial of Jamf today.

Request Trial

Or contact your preferred Apple reseller to get started.