Modern Management

The Future of MDM

The best IT managers know their tech inside and out. They know that the most effective technology is chosen after careful consideration of what will support an organization's employees and its unique business objectives. Moreover, they understand that while they support the workplace of today, they must be ready to adapt to changing needs in the future. This means embracing and empowering hybrid work by adopting modern device management practices that enable employees with a secure and seamless device experience, from anywhere.

In an Apple environment, ingenuity races ahead, with Apple itself leading the charge. They continue to innovate to meet the needs of the enterprise. Keeping pace means meeting the challenge of supporting a mobile workforce and satisfying user demands at Apple's speed.

Studies show that flexible organizations have lower operational costs, attract and retain the best talent and see an uptick in employee productivity when they move to hybrid or remote practices.

MDM providers like Jamf, situated at the intersection of Apple and the enterprise, strive to take Apple's innovations and enable them to be distributed and maximized on an enterprise scale. This necessitates ensuring that strategies reflect the future's needs.

> **"Today's best experience is tomorrow's expectations"**
>
> **— Fletcher Previn, CIO at Cisco**

source: Mac in the enterprise: Drive the future of work with employee choice

What is Modern Management?

Modern management combines the management and security of devices, users, operating systems, and applications from the cloud. Going far beyond traditional Mobile Device Management (MDM), modern management can be considered the next evolution of endpoint management and security. This approach offers a holistic perspective by integrating these elements, resulting in enhanced security, management, and situational awareness for IT departments, enabling more responsive actions.

In short: adopting and strategizing around modern management practices with Apple means that employees have a secure and seamless device experience from anywhere they work. It means IT has the tools and systems in place to support and execute at the pace the modern workplace demands.

This next evolution should lead organizations to think about their Apple environment and ask:

- Do we have a strategy that reflects a modern way of managing and securing devices?
- What are the gains from adopting modern management?
- What are we losing if we don't keep up?

A History of Traditional Apple Management

IT admins have been stead-fast in following traditional or legacy management for years, which, up until recently, made sense for the workforce. Traditional management operates on a device-centric model, wherein corporate-owned devices are assigned to employees, and only these authorized devices can access the company's on-premise network for essential applications and services. However, in today's dynamic work environment, this approach falls short of meeting employee needs.

To better understand Apple's evolution in addressing these challenges, let's examine the history of managing Apple devices.

Before Mobile Device Management (MDM): the binary

Before Apple released their MDM protocol in 2010, the only Apple device that organizations were managing was macOS. At the time of enrollment, those managed Macs would get some local binaries, those local binaries would have root privileges, and they would be able to retrieve data about the Mac to send back to a management server, on a defined schedule. They'd also be able to tell the local client to take programmatic action by downloading packages and running local scripts. **This was called 'forced pull' device management**.

There's no denying that during this time, macOS device management required an enormous amount of IT resources.

Early MDM: focus on devices

Then iPhone came onto the scene and changed the MDM style. Gone was an agent with root-level access, periodically contacting a management server. MDM necessitated push notifications.

Traditional MDM relies on a device maintaining a persistent connection to Apple and a management server asking Apple to have a managed device 'phone home' to obtain a setting, receive a command or query or install an app.

Here is an example of what that might look like:

1. The command could be *"update your OS."*
2. Then the subsequent query might be, *"What's your current OS?"*
3. An admin might then ask again to ensure the command went through correctly: *"How about now?*

...No update? I guess you'll be checking again tomorrow.

Traditional MDM means admins get acknowledgments when commands have been received or completed, and they can request and receive a substantial amount of information from the device. **But the admin has to ask, and ask repeatedly.** Sometimes, that means getting a lot of duplicative information back. For commands that are complex or contain conditional workflows, the flow of information back and forth increases. Asking your management server to parse that information and, potentially, perform calculations against the changes can trigger resulting commands and queries.

With more personally-owned devices showing up in the workplace, BYOD workflows with User Enrollment have a deliberately limited subset of MDM functionality and visibility. Managed Apple IDs are unlocking new workflows. The complexity of device management has increased significantly. **It's not as cut and dry as it used to be: full management or nothing at all.**

Fortunately, throughout the past 20 years, the protocol has gotten some new tricks with more commands and granular settings. All of this has led to Apple's Declarative Device Management (DDM) protocol.

Harnessing Innovation: Declarative Device Management

Declarative Device Management has been positioned as the future of device management. It is also a critical enhancement to aid in streamlined security workflows. Declarations can send far more detailed, up-front instructions that tell the device how to behave under a set of conditions. That set of instructions combines with status reporting to alert the management server when certain values change on the device.

In other words, a device proactively takes action if it falls out of compliance and can send updated information directly to the server. It doesn't have to wait for the server to ask them for a report, report the issue, and then wait for the server to tell it what to do. **As a result, device information is more accurate and policies to keep a device compliant can work faster.** This also cuts down network traffic considerably, resulting in a marked increase in performance and speed.

Declarative Device Management marks a trend in the shift to modern management. Through enhancements in Declarative Management, MDM will empower administrators to craft more intricate and innovative strategies. This will simultaneously bolster device security by default, while ensuring prompt notifications for staff when vital conditions change.

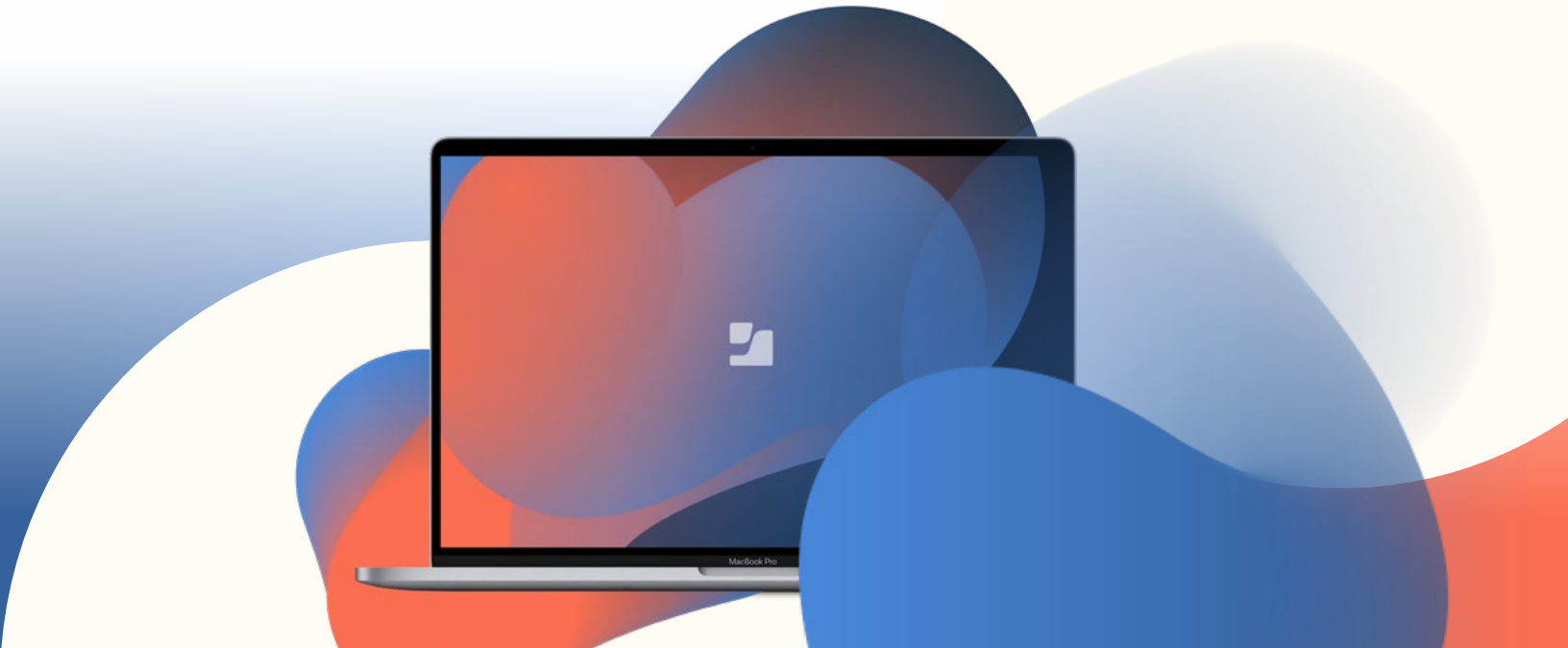
MDM will be:

1. **More secure** by permitting declarations to set compliance out of the box and limiting programmatic interactions with low-level binaries
2. **More native** by enabling end-user interactions based on declarations
3. **More useful** by iterating on the already strong foundation of MDM with DDM

Benefits of a Modern Management Strategy

As hybrid work continues to be the norm for—and the expectation from— our employees, how we provide access to the tools they need to innovate, create, and collaborate successfully has evolved. **Users want a dynamic experience that focuses on providing them with the data and tools they need, from almost any location, using the entire Apple ecosystem.**

Operating system, application software, and security updates routinely deliver new features, functions, and protections aimed at improving the experience of users and protecting devices from attacks. Today's faster development cycles and feedback loops



make it easier to push updates to users quickly. As a result, a device may be subject to multiple updates per week, and that can interrupt the end user experience. Users want to take advantage of updates, features, and performance and security enhancements. But they do not want a device to tell them to stop and reboot when they are in the middle of a critical project or their most productive working hours.

This means a migration from the traditional, on-premise structure to a modern, cloud-based system that effectively manages and secures any Apple device type, anywhere.

Moving to the cloud allows organizations to move faster and offers flexible resources, how and when users want them, compared to on-premises resources. Modern tools automate routine IT functions, reducing the burden of time-consuming IT tasks and allowing admins to spend time focusing on other specific issues. Self-service tools help end users and IT by reducing the need for IT to initiate tickets or reset passwords, and by offering employees immediate access to apps and information.

Cloud deployments also offer a number of security advantages over on-premises deployments. In particular, cloud security features and services such as:

- Verified enrollment to trust the integrity of every device managed within your organization, leveraging built-in enrollment methods like automated and user enrollment
- Identity and access management to control who has access to what resources based on an individual's cloud identity, helping to prevent unauthorized access to sensitive data and applications
- Privilege management to give users only as much access as they need to sensitive data parts
- Granular access policies for apps & data to ensure that only authorized users on sanctioned (managed) devices are able to access work apps and data
- Secure network traffic to ensure that all work traffic is securely encrypted to prevent unauthorized access
- Conditional access providing real-time security data from managed devices that continuously evaluates risk signals and automatically limits access to work resources based upon customizable risk thresholds

An increasingly distributed workforce, using a broad range of devices, presents many challenges. Embracing modern management practices means you're more than up to the challenge, enabling a consistent experience for both the users and the IT teams.

The best way to adopt modern management for Apple is with Jamf

Jamf has been around in Apple MDM for a while, more than twenty years. Our close working relationship with Apple means that when they deploy a new release, we support it from day one.

But in the world of tech, more than twenty years can feel like a lifetime. That may tempt some people to think we're settled a bit in our ways. **But Apple continues to innovate, and Jamf right along with it.** Both organizations have undertaken a journey into state-of-the-art management, which has resulted in a complete transformation of how device management and security works.

Jamf emerged as a leader in transitioning to cloud-based solutions. This shift was driven by the recognition that as the number of devices within an environment grows, there's a corresponding demand for scalable, globally-accessible services to effectively manage them. So Jamf offers the ability to host your Jamf Pro MDM server with **Jamf Cloud**.

Along with hosting your server in the cloud, **Jamf Pro** offers a number of cloud-based features such as **App Installers**, **Jamf Cloud Distribution Service** and **Managed Software Updates via Declarative Device Management.**

Software update management is a core feature of device management and we know this is something our community needs. Thanks to the close working relationship with Apple, Jamf was ready to hit the ground running with managed software updates via DDM. Admins in Jamf Cloud can now schedule and enforce software updates to be completed by a specific date and time. Thanks to DDM, those updates will automatically be applied to all of the respective Mac and mobile devices. Not only will support for this workflow improve the software update experience for admins and reduce reliance on third-party tools, but it will also help devices stay compliant with the latest OS updates and security fixes.

To ensure that only authorized users are accessing corporate resources, **Jamf Connect** integrates with cloud identity providers for modern, secure Mac authentication with just-in-time local Mac account provisioning and password sync. A user can unbox their device, power it on and access all of their corporate applications and resources after signing on with a single set of cloud identity credentials - anytime, from anywhere.

Revolutionize with a Modern Management strategy: Unleash the possibilities of your Apple ecosystem

A cloud environment coupled with Declarative Device Management means a faster, smoother and more secure way to manage and secure your devices. It offers the user experience that the modern workplace needs while removing the IT burdens of traditional management.

If you're ready to **join Apple and Jamf** on the transformative journey to **modern management**, and you want to take advantage of all that the cloud and DDM has to offer, **we can help!**