



# The Whys and Hows of **Apple** Enterprise Management





In our e-book, *How Apple Enterprise Management Goes Beyond Mobile Device Management*, we introduced you to what **Apple Enterprise Management** is and why a scalable and automated solution dedicated to Apple hardware and software is what your organization needs.

Dive deeper with this e-book into the **whys and hows around connecting, managing and protecting your Apple fleet**. We'll cover why Apple Enterprise Management is the way forward in the enterprise, its solutions and capabilities, and how to transition from mobile device management (MDM) to Apple Enterprise Management.

**Apple Enterprise Management** is zero-touch deployment, identity-based access and management, inventory management and reporting, security compliance and reporting, automated device management, application lifecycle management — all working together to support employee productivity, efficiency and experience.

## Why? Because...

Organizations are considering new ways to support employee productivity and wellness — giving employees flexible work options and work/life balance for happier, more productive employees.



Data-driven methodologies are shaping business decisions, and organizations are increasingly relying on multiple data sources to evaluate efficiency and areas for improvement and optimization.

Organizations need to have iron-clad security protocols in place to ensure security and privacy for devices, users and their corporate data — especially as hybrid and mobile workforces are established as enterprise norms.

## How? **It's simple.**

---

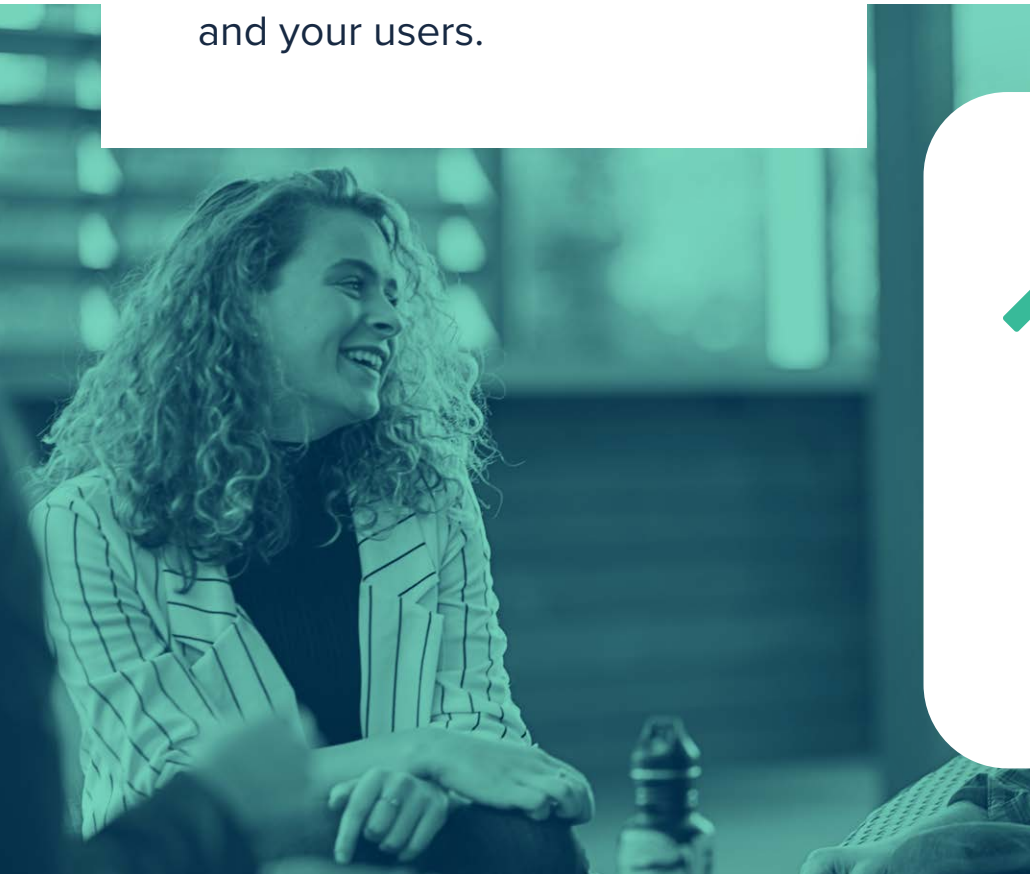
Connect users to the resources they need, manage hardware and software with the user experience prioritized at the forefront, and protect your fleet and your users.



### **Empower**

users with the ability to set up their devices and gain instant, identity-based access to corporate resources, content and trusted apps through a single click — all while keeping their username and password in sync.

**CONNECT**





CONNECT



## Integrate

with Apple deployment programs to automate enrollment and custom configuration to deliver a scalable, zero-touch experience for personalized onboarding. Add bookmarks, policies and workflows, like cleanup scripts and even VPN configurations, to your organization-branded Self Service app portal, giving employees immediate access to the resources they need to be successful.



## Embrace

a true Zero Trust Network Access (ZTNA) solution. With Jamf Private Access, you can replace legacy conditional access and VPN technology. With ZTNA private access, after a user authenticates into their device, business connections are secured while enabling non-business applications to route directly to the internet, preserving end-user privacy and optimizing network infrastructure.

Whether leveraging Jamf Connect, Jamf Private Access or harnessing the power of both solutions, the safety of your data, resources and users — and their experience — is essential in the enterprise.



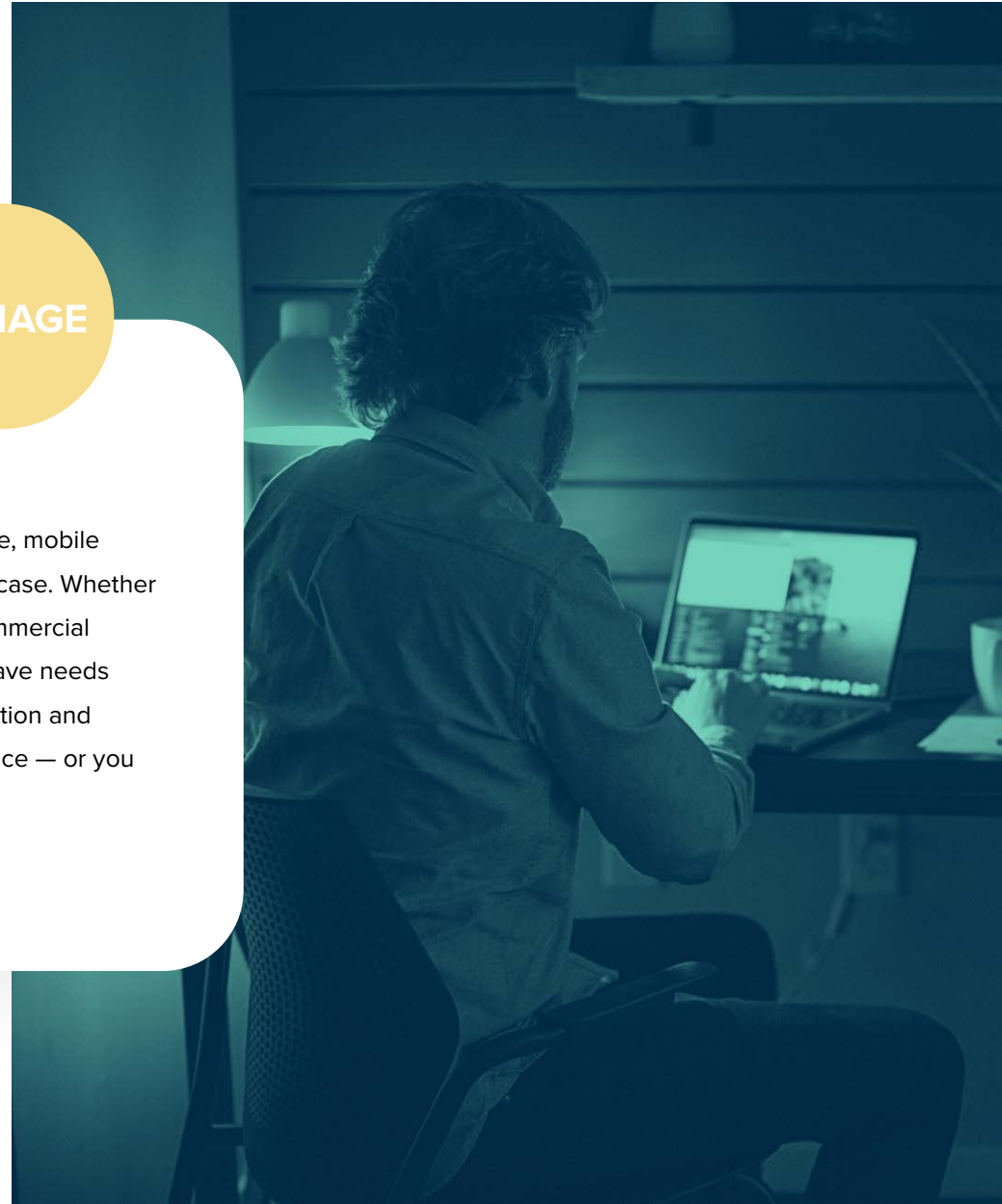
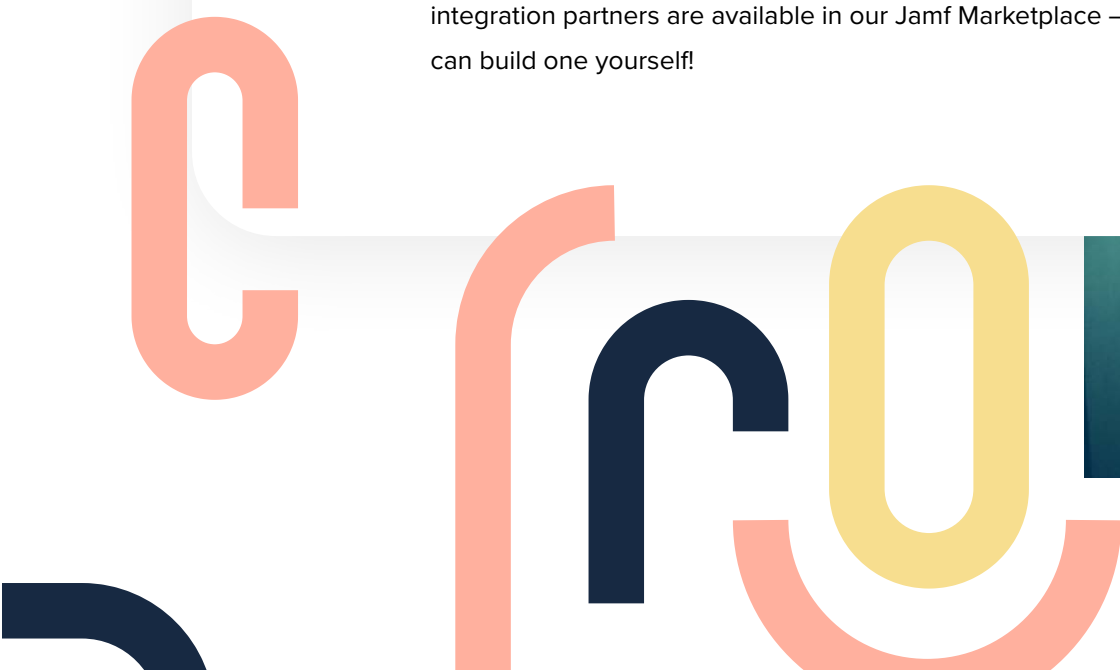


## MANAGE



### Maximize

your investment with Apple and accommodate a flexible, mobile workforce with industry-specific workflows for any use case. Whether your organization is in healthcare, hospitality or the commercial space, tailor-made solutions are available. And if you have needs that aren't met with pre-designed solutions, Jamf's solution and integration partners are available in our Jamf Marketplace — or you can build one yourself!



MANAGE



## Automate

enterprise needs — from workflows related to the installation and ongoing management of applications to inventory management and identity management — to optimize spending and lower operational costs.



## Enforce

consistent policies for better and more cost-effective management. With Jamf Data Policy, you have another layer to Jamf's management capabilities including data capping, content filtering and more.

Managing your Apple enterprise fleet with Jamf ensures that your hardware, software and end users are functioning efficiently, effectively and safely without sacrificing the native Apple experience.

# PROTECT



## Fulfill

your requirements around access and security without compromising enterprise and end-user privacy.



## Restrict

malicious software and patch all of your Apple devices without any user interaction and manage device settings and configurations by working with native Apple encryption features.



## Isolate

and remediate macOS vulnerabilities proactively for known and unknown malware. And with multi-factor authentication (MFA) enabled for each and every login, rest easy knowing the right person is accessing the machine and resources.







## PROTECT



### Audit

against security benchmarks like Center for Internet Security (CIS) Benchmarks and enforce compliance with enterprise security requirements.

Jamf Threat Defense protects iOS endpoints from being compromised through mobile threat detection and zero-day phishing prevention with a first-class app for notifications and remediation.

Together, Jamf Protect and Jamf Threat Defense are a complete purpose-built solution to protect Apple users from malicious intent — all while maintaining minimal impact on the end-user experience.

Jamf — the standard in **Apple Enterprise Management** — is the only solution of scale that automates the entire lifecycle of Apple in the enterprise, including device deployment, management and security, without negatively impacting the end-user experience or requiring IT to touch the device.

Jamf preserves the native and consistent Apple experience that people expect at work while fulfilling the security, compliance and privacy requirements of the enterprise. And we're here to help you embrace and implement **Apple Enterprise Management**.



If you're starting from square one and want to see what's possible with Jamf:

[Request Trial](#)

Or ask your preferred **Apple reseller** to get started with a free trial.

If you're already a Jamf customer and are looking to extend the power of your solution with the Apple Enterprise Management platform:

[Contact Your Sales Rep](#)



If you have a UEM solution or a non-Jamf MDM solution, here's a checklist for what to do next:



### **Assess your current management solution**

Are you trying to manage devices across different ecosystems with one solution, aka unified endpoint management (UEM)? See why UEM isn't the best approach to managing your enterprise.

[Why Unified Endpoint Management \(UEM\) Falls Short](#)



### **Learn how to migrate to a new MDM solution**

Change is hard, but that's rarely a good reason to continue with the status quo. Migrating MDM solutions doesn't need to be the stop-gap for you. Here's a step-by-step guide for how to switch solutions.

[A Migration Guide For Businesses Switching Mobile Device Management Solutions](#)



### **View the business plans & pricing**

Jamf provides complete Apple Enterprise Management across the Apple Ecosystem with Jamf Pro, Jamf Connect and Jamf Protect capabilities — and support and training for your enterprise. Learn about plans and pricing at [jamf.com/pricing/](https://jamf.com/pricing/)



### **Contact us**

Complete Apple Enterprise Management across the Apple Ecosystem with Jamf Pro, Jamf Connect and Jamf Protect capabilities — and support and training for your enterprise — isn't too good to be true. Contact us to see what the Jamf Business Plan and Apple Enterprise Management can do for you.

**Get Started with Jamf**