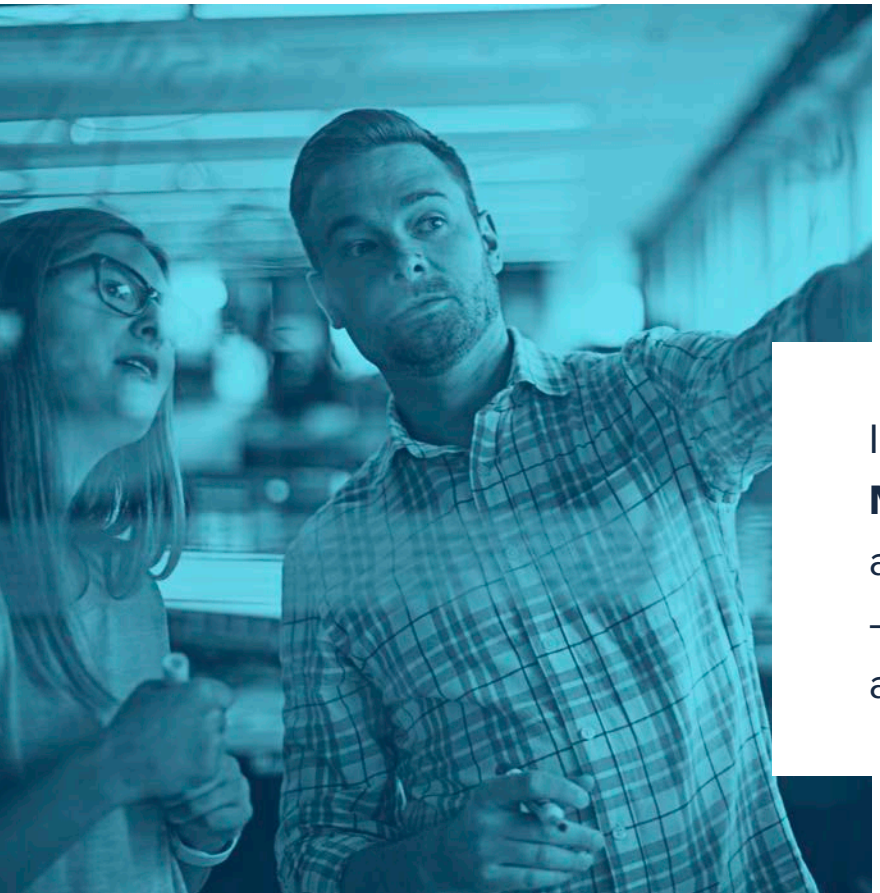
How Apple Enterprise Management Goes Beyond Mobile Device Management

jamf

A better way to maximize Apple

No enterprise tool has successfully supported the vast and varying needs of the modern enterprise technology fleet, which often is comprised of a mix of Apple, Microsoft and Google devices.



Each ecosystem has unique workflows for provisioning, deploying, securing and updating enterprise technology. And in a world with increasing remote workforces, new obstacles and growing pains are to be expected. But with the right enterprise management solution — specifically tailored to the nuances of each ecosystem and its respective users — you can support your employees and enterprise across all of the variables and needs of an evolving workforce.

In this e-book, we introduce you to **Apple Enterprise Management** and explain why a scalable and automated solution — designed specifically for Apple — is the best method to connect, manage and protect an entire Apple fleet.

What is Apple Enterprise Management?

The vision of unified endpoint management (UEM), where all devices are managed by a single tool, has failed to be successfully implemented by most enterprise organizations. In fact, a Forrester Research analyst cites less than 5% of organizations are adopting modern management solutions or leveraging UEM.

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.

With every Apple device, organizations need to be able to seamlessly incorporate technology that drives business initiatives by offering users secure access to the resources they need, empowering IT to deliver the functionality required in today's modern work environment, and providing Information Security teams with the peace of mind that devices and data are protected at all times — all while delivering an exceptional experience for every employee.

Apple Enterprise Management achieves this by automating and supporting the entire lifecycle of Apple in the enterprise:

- **Zero-touch device deployment**
- **Account creation, authentication and identity management**
- **Device and app management**
- **Security planning, detection, reporting and remediation...**

...all without negatively impacting the end-user experience or requiring IT to touch the device.

And since **Apple Enterprise Management** is solely focused on Apple devices, enterprise organizations are empowered and invariably ready to support and extend Apple's latest operating system functionality. As a result, organizations can upgrade to latest Apple operating systems with all of their new features and security mechanisms the day they ship from Apple.

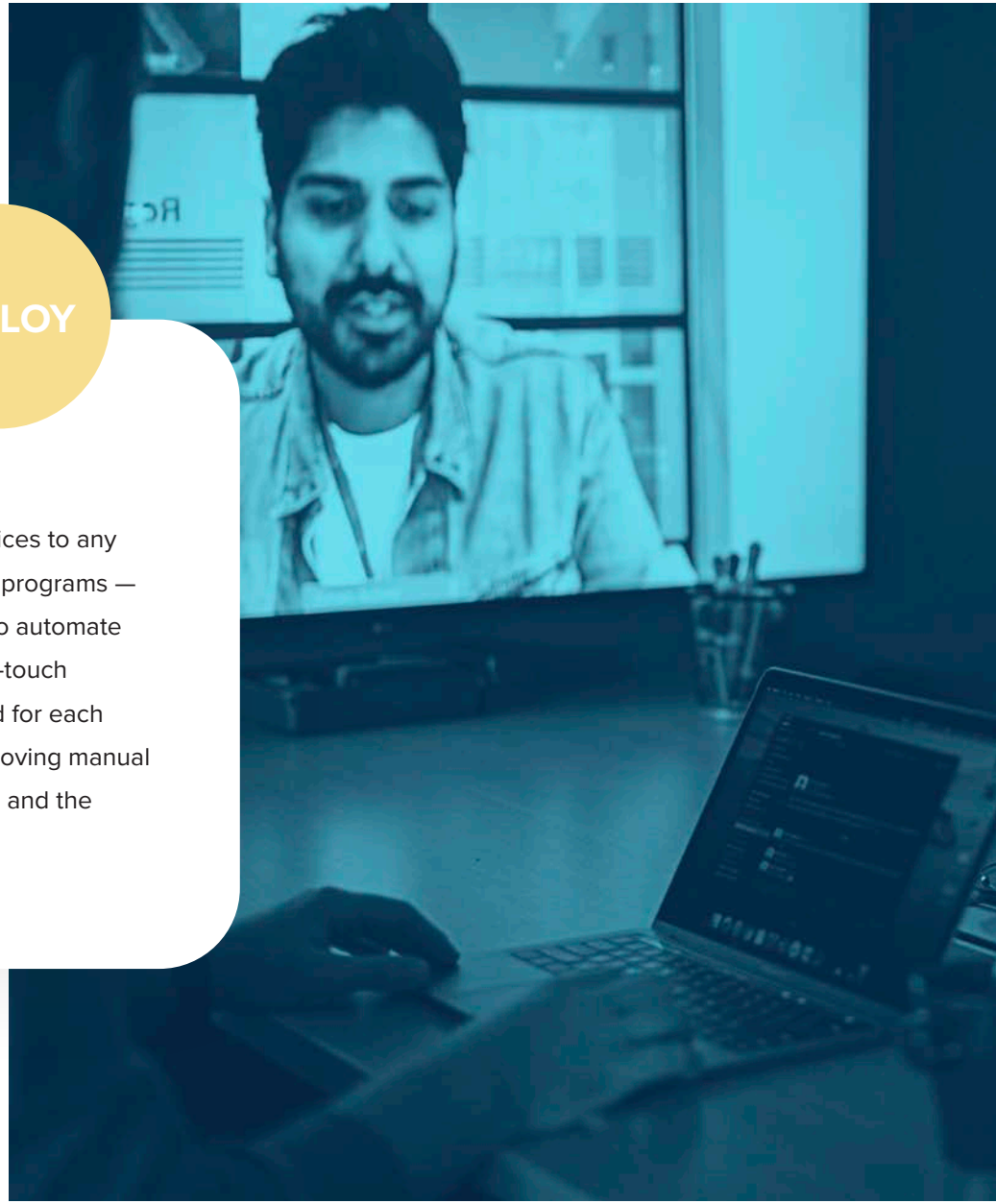
How is Apple Enterprise Management different from mobile device management?

Simply managing Mac, iPad, iPhone and Apple TV is no longer enough for modern enterprises, and leaves IT, Information Security and other critical teams lacking tools to:

- **Securely connect users to resources they need to be productive and self-sufficient**
- **Automate every aspect of device and application management**
- **Adequately protect devices, data and user privacy**

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.

How does Apple Enterprise Management work?



DEPLOY

Zero-touch deployment

With zero-touch deployment, you're able to deploy devices to any employee, anywhere. Integrate with Apple deployment programs — Apple Business Manager or Apple School Manager — to automate enrollment and configuration providing a scalable, zero-touch experience with each shrink-wrapped box, personalized for each individual — and save yourself tremendous time by removing manual tasks in the process. Getting started is easy, accessible, and the experience end users expect from Apple.

Whether onboarding new employees and setting them up for their first day or managing ongoing support for your workforce, you can find comfort knowing your users have secure access to your network and resources.

CONNECT

Identity-based access

Provision devices with business-critical applications needed to be productive based solely on an employee's cloud-identity credentials. Users will enjoy a seamless experience when accessing their device and applications with a single password that is synchronized down to the local-account level, even when the password is changed, keeping employees on task. And with multi-factor authentication enabled for every login, rest easy knowing that only the right person is accessing the machine and resources.

Curated resources on demand

Add bookmarks, policies, workflows like cleanup scripts and even VPN configurations to a branded Self Service app portal to give employees instant access to resources they need. Employees can troubleshoot common issues in one click, drastically reducing help desk tickets for IT.

MANAGE

Device management

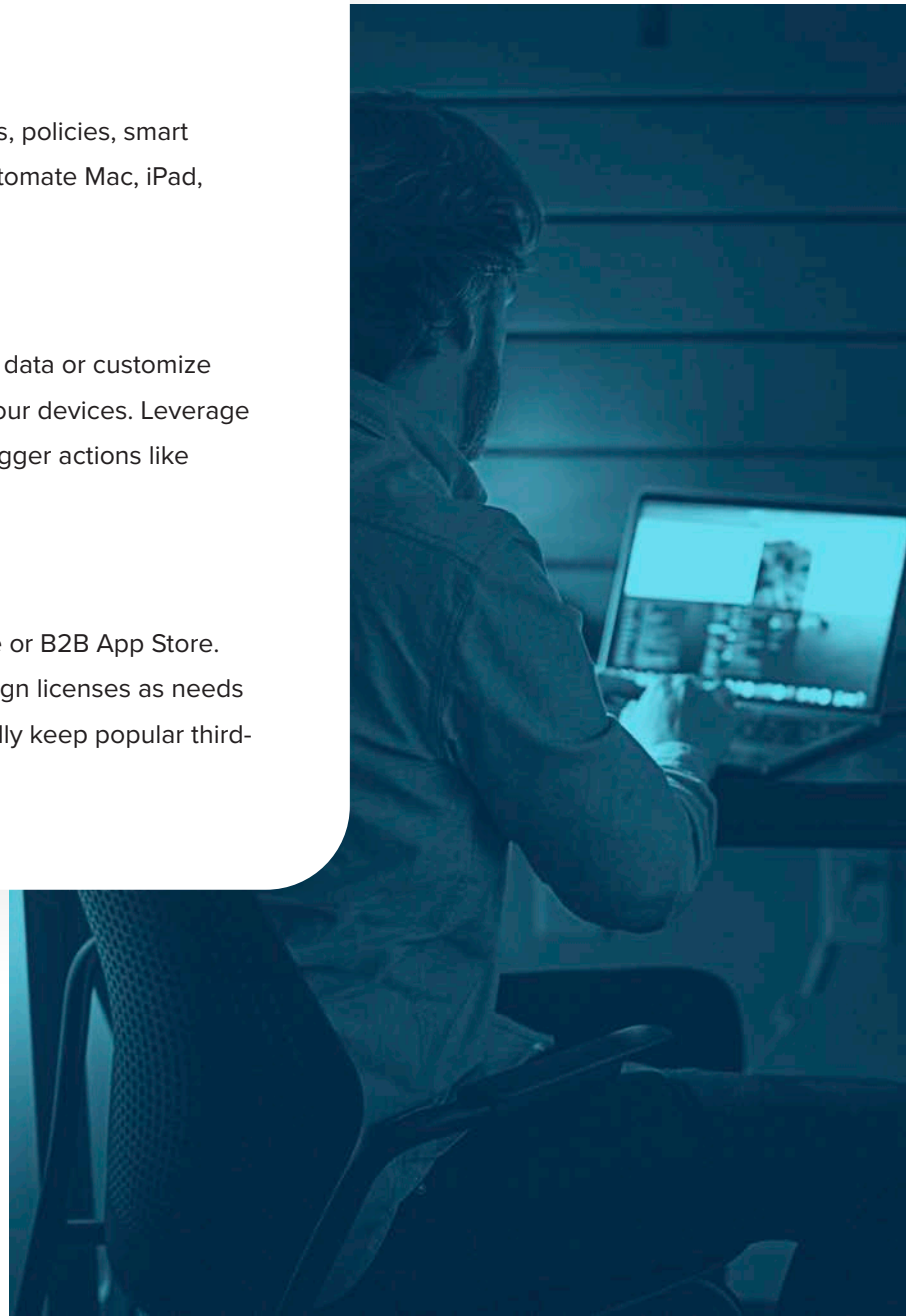
Through remote management and the use of configuration profiles, policies, smart targeting and scripts, you can leverage advanced workflows to automate Mac, iPad, iPhone and Apple TV management.

Inventory management

Automatically collect user, hardware, software and security device data or customize inventory specifications so you always have a bird's-eye view of your devices. Leverage rich inventory data and patented Smart Groups to automatically trigger actions like operating system upgrades.

Streamlined app management

License, deploy and manage apps in bulk right from the App Store or B2B App Store. Assign apps to users or devices (no Apple ID required) and re-assign licenses as needs change. Build custom app and software packages and automatically keep popular third-party software titles up to date.



MANAGE

Partners and integrations

Jamf solutions fit seamlessly into your existing technology stack by offering out of the box integrations, as well as robust APIs. This programatic access to Jamf powers hundreds of integrations found on the Jamf Marketplace. These technology partners are driving not only new use cases for Apple devices, but efficiencies for administrators and end-users alike.

Co-management with Microsoft

Conditional Access for Mac and Device Compliance for iOS allow organizations to share important Apple device information — like compliance status — with Microsoft Endpoint Manager. This ensures only trusted users from compliant devices, using approved apps, are able to access company data.

Industry-specific workflows

Customized workflows like Healthcare Listener, which digitally sterilizes iPad upon discharging a patient, address and solve issues specific to your organization or industry's needs that are not met with simple device management.

Apple Enterprise Management automates management of user devices and apps to streamline and support your organization, devices and end users.

PROTECT

Threat prevention and remediation

To ensure privacy and speed, real-time alerts analyze activity on-device and proactively block, isolate or remediate threats leveraging the same tooling you use to manage the device. Prevent, detect, and remediate malware and attacks that target Apple devices, instead of impacting the end-user experience searching for Windows attacks on Apple devices.

Security management

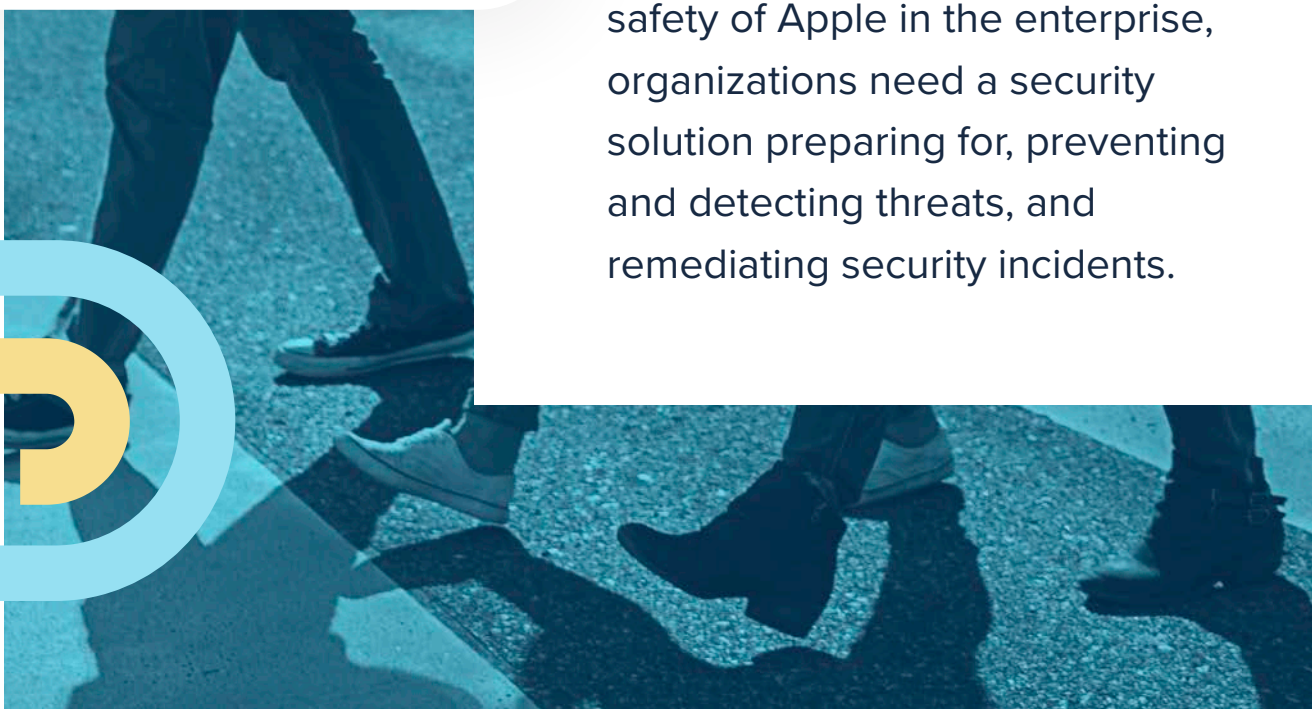
Ensure your devices maintain a strong security posture by implementing OS hardening benchmarks for Apple devices. Apple Enterprise Management leverages native Apple security features such as enforcing encryption on macOS and passcodes on iOS, runs policies to enforce FileVault encryption on macOS, restricts malicious software and patches all of your Apple devices without any user interaction. Apple Enterprise Management also ensures that any devices that stray from these benchmarks are quickly identified and brought back in compliance.

PROTECT

Broad security and compliance visibility

With dashboards, real-time alerts, as well as extensive reporting on file, process, malicious activity on macOS devices and built-in tool activity from macOS security frameworks like XProtect, Gatekeeper and MRT, you have the data at your fingertips to identify and investigate any security incidents. To complement this low-level security data, Apple Enterprise Management gives you full insights into device logs for higher-level security data and compliance insights.

With Apple device adoption on the rise, protecting your fleet with a security solution designed specifically for Apple has never been more important. To ensure the success and safety of Apple in the enterprise, organizations need a security solution preparing for, preventing and detecting threats, and remediating security incidents.



Conclusion

From the first point in a device's lifecycle though the ongoing support and security of maintaining your fleet, **Apple Enterprise Management** is the missing piece to empowering your IT and Information Security teams, as well as your end users.

Deploy, connect, manage and protect your Apple fleet and corporate resources with all that Jamf has to offer.

jamf

See the benefits of Jamf's **Apple Enterprise Management** solution for yourself.

Get Started

Or contact your preferred reseller of Apple to get started.