

# How to Empower a Remote Workforce



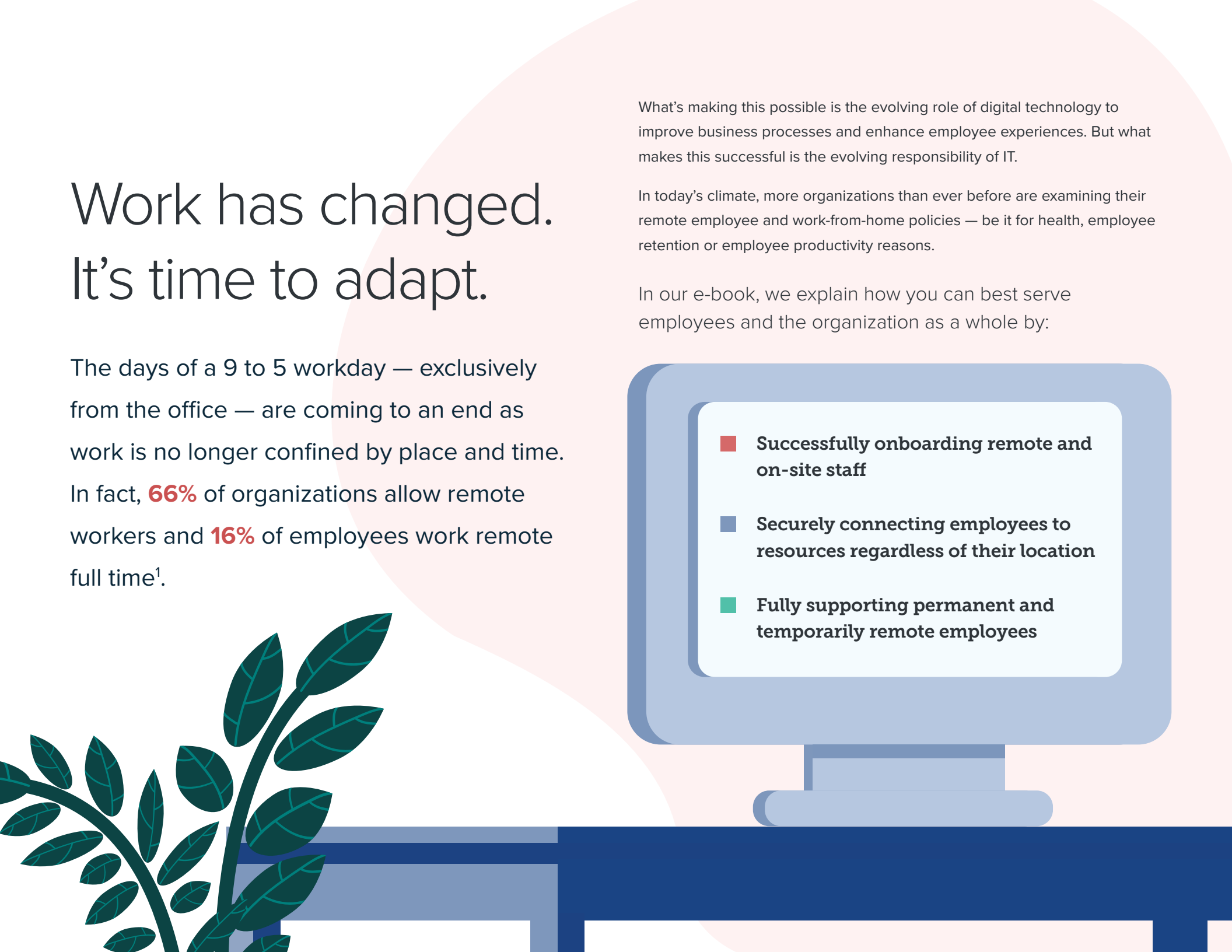
# Work has changed. It's time to adapt.

The days of a 9 to 5 workday — exclusively from the office — are coming to an end as work is no longer confined by place and time. In fact, **66%** of organizations allow remote workers and **16%** of employees work remote full time<sup>1</sup>.

What's making this possible is the evolving role of digital technology to improve business processes and enhance employee experiences. But what makes this successful is the evolving responsibility of IT.

In today's climate, more organizations than ever before are examining their remote employee and work-from-home policies — be it for health, employee retention or employee productivity reasons.

In our e-book, we explain how you can best serve employees and the organization as a whole by:

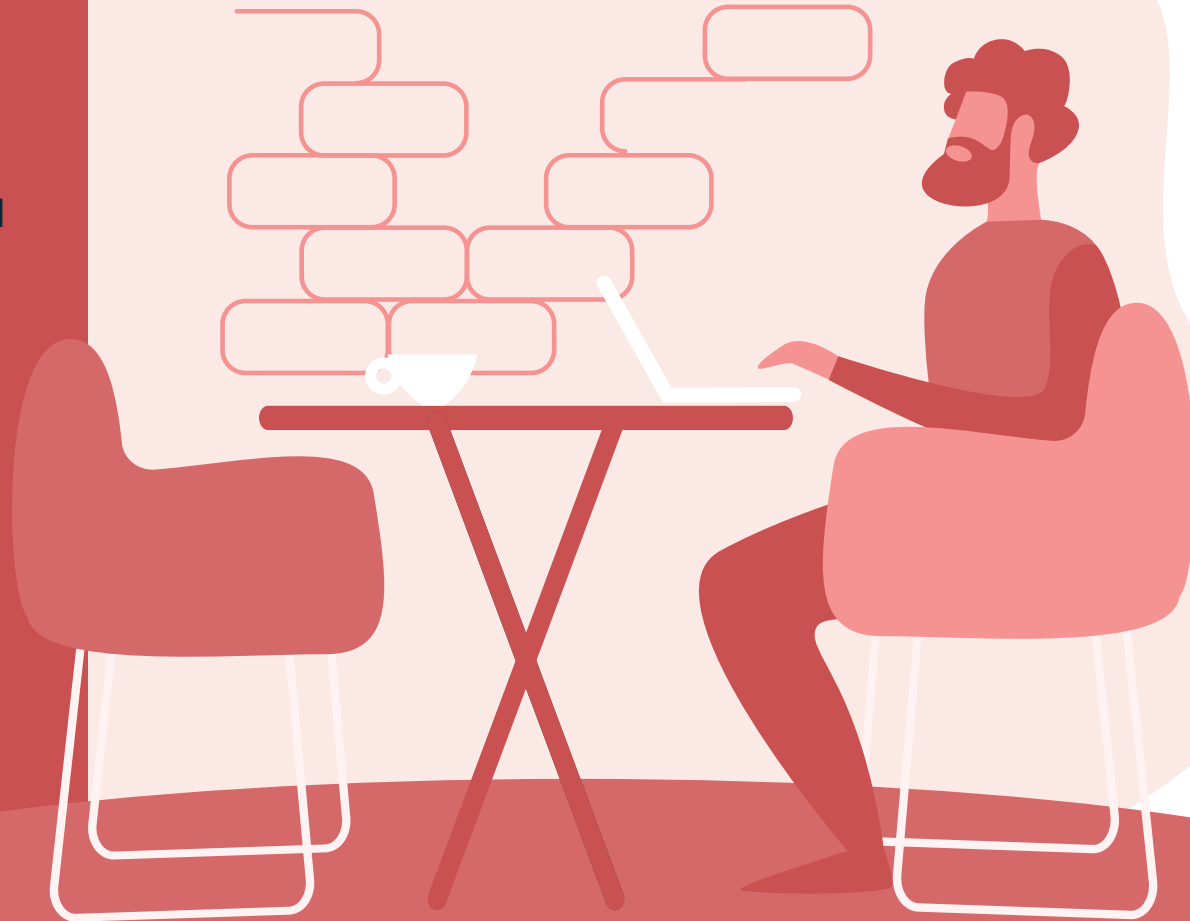
- 
- **Successfully onboarding remote and on-site staff**
  - **Securely connecting employees to resources regardless of their location**
  - **Fully supporting permanent and temporarily remote employees**

# Better onboarding experience for all

The speed at which organizations must empower employees to be productive is directly correlated to the retention rate and level of productivity of new hires. When organizations deliver a strong onboarding experience, they can improve employee retention rates by **82%** and employee productivity by over **70%**<sup>2</sup>.

So, it is paramount that organizations are offering the right technology and leveraging the right tools to facilitate a streamlined onboarding process for remote and on-site employees. But when it comes to choosing how to best support those goals, not all technology and tools are created equal.

Apple hardware is becoming much more common place in enterprise organizations around the world. The ease of use and [growing employee demand](#) are opening the eyes of many organizations to support and offer Mac, iPad and iPhone. And, this trend has tremendous benefits for employees, IT and the entire organization.



## Efficient onboarding for IT

IT only gets one chance to make a good first impression. They can nail theirs by leveraging **Apple Business Manager** to institute a company-wide zero-touch device deployment strategy. When a new device is unboxed and powered on, Apple Business Manager tells the Mac, iPad or iPhone to automatically enroll into the organization's mobile device management (MDM) solution.

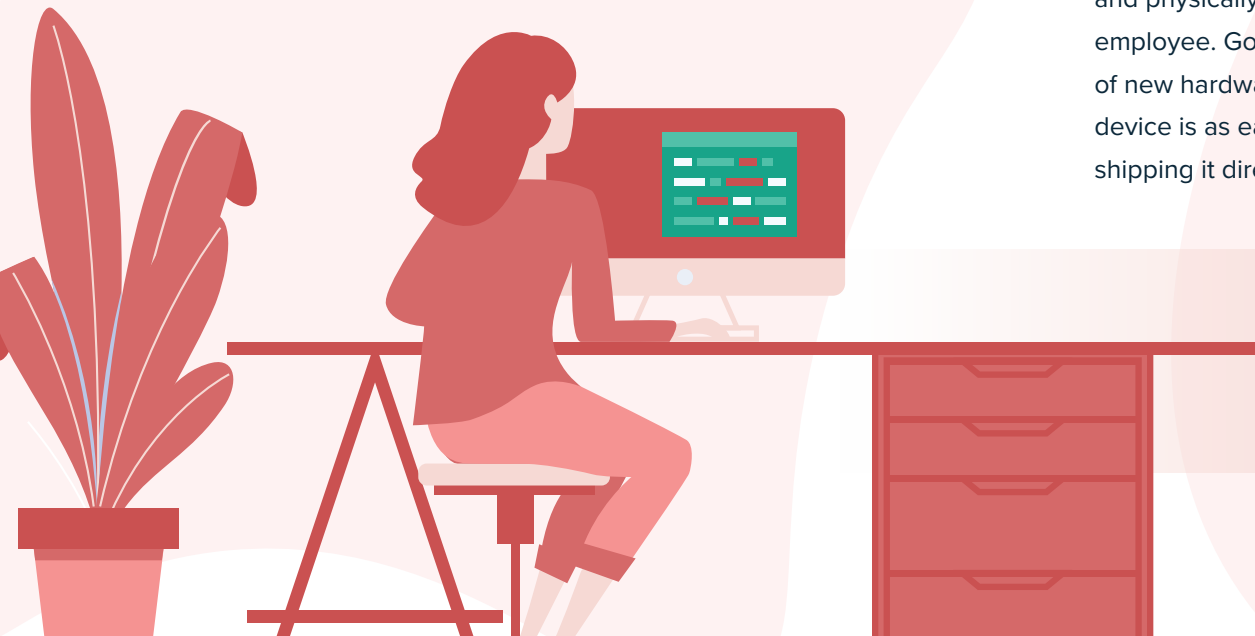
**Jamf Pro** — the gold standard for Apple enterprise management — is built from the ground up to deeply support Apple Business Manager and take it to the next level. With powerful technology like Smart Groups — which help intelligently manage environments without any interaction — Jamf Pro is the best platform to support a growing remote workforce. For small businesses, Jamf offers **Jamf Now** — mobile device management built for anyone.

Apple Business Manager — a free service from Apple — also helps streamline the process of Apple IDs, when paired with a management solution like Jamf Pro or Jamf Now. Leverage Managed Apple IDs and be fully in charge of the set up and management of the Apple ID. Employees benefit from an Apple ID strategy that is clearly designated for work, eliminating any confusion about whether they should use their personal Apple ID in the workplace. Admins will enjoy fewer support tickets as end users are empowered to manage and reset their own passwords without needing IT support.

This workflow completely eliminates the process of unboxing each device and physically touching it to get it personalized and configured for each employee. Gone are the days of IT needing to be buried under a mountain of new hardware. With Jamf and Apple Business Manager, deploying a new device is as easy as ordering it via the Apple Business Manager portal and shipping it directly to an end user's desk or home.



No further IT interaction is needed, so you can get back to supporting your distributed workforce in other ways.



# Better onboarding experience for all

To institute the zero-touch deployment process, all organizations need to do is **prepare**, **purchase** and **deploy**.

## Prepare

- 1 Sign up for Apple Business Manager
- 2 Link Apple Business Manager account to the MDM server
- 3 Configure settings and enrollment customization



## Purchase

- 1 Order Apple hardware through Apple or an authorized Apple reseller
- 2 Assign devices for enrollment



## Deploy

- 1 Send shrink-wrapped Apple devices directly to employees
- 2 Employee unboxes and turns on
- 3 Apple device enrolls into management automatically



## Easy onboarding for employees

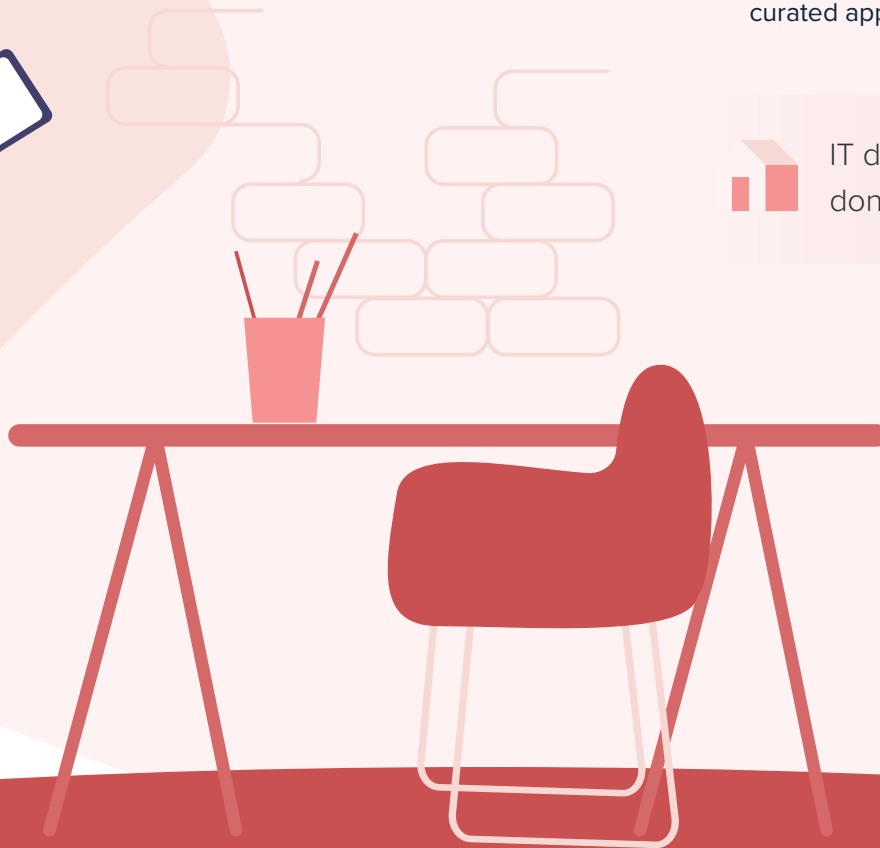
First days are inherently stressful for employees. Alleviate their concerns by getting the tools they need (and want) in their hands-on day one through a zero-touch deployment.

For a remote employee, productivity is literally a few taps or clicks away. They simply look for their new Apple hardware in the mail, unbox it and power it on. That's it! Employees become instantly connected to their work resources, including mail, VPN and productivity apps in the same exact manner as their on-site counterparts. Your device management solution should also allow for flexible configuration of the Enrollment Customization workflow, making it easy for you to provide video, documentation or other information as a new employee clicks through the enrollment screens on their device.

Once online, remote employees are able to quickly find and take advantage of their favorite apps or other critical resources thanks to Self Service, a free curated app portal available to every end user in the organization.



IT doesn't have to touch any devices and employees don't have to step foot in an office to get their hardware.



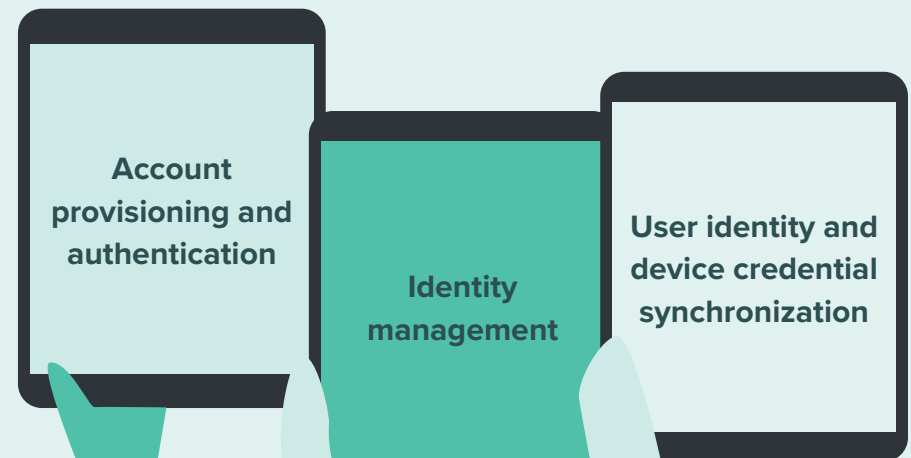
# Connecting employees through zero-trust access

To further differentiate and customize the device deployment process and ongoing lifecycle management for remote and on-site staff, organizations are turning to modern authentication and security measures.

Through an authentication and identity management solution such as [Jamf Connect](#), organizations can implement a “never trust, always verify” strategy. This is crucial for remote staff who are potentially accessing secure information and resources over unsecure networks.

Jamf Connect and cloud-identity providers — such as Okta and Microsoft Azure Active Directory — offer organizations a high level of user and device trust, while also ensuring a seamless and uninterrupted experience for employees.

This is accomplished through three areas:

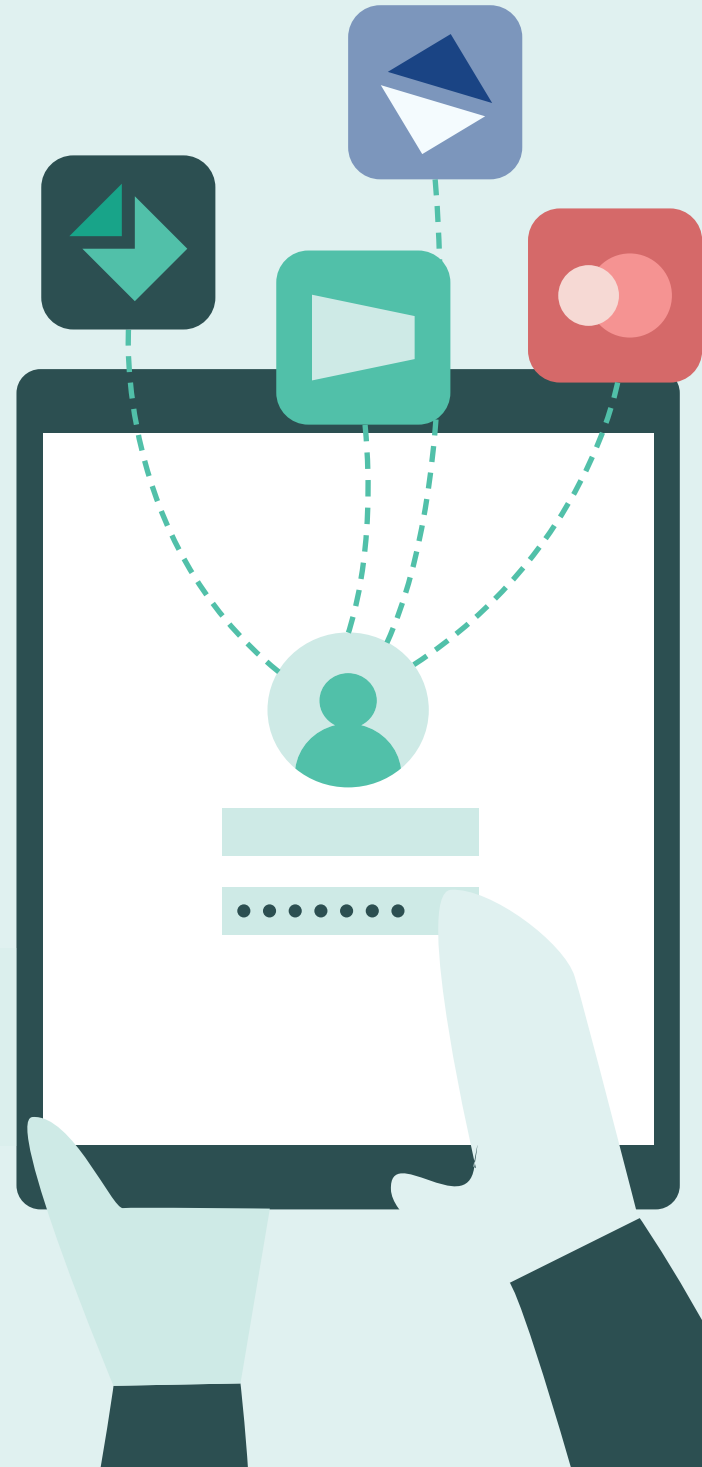


## Account provisioning and authentication

IT administrators can provision a Mac with all of the business-critical applications needed to be productive based solely on an employee's cloud-identity credentials. This takes zero-touch deployment one step further as the user can login with a single set of credentials, complete with multifactor authentication, so the organization knows the right person is accessing the right machine and the right resources.



For day-to-day operations, this simple yet secure login experience is leveraged every time a user logs in.





### Identity management

Because Jamf Connect requires a cloud-identity username and password, IT administrators are able to monitor what devices are being accessed, from where and by whom. This is a powerful security measure to keep remote employees protected as they may be logging into their device from an unsecure network or if a device is lost or stolen.



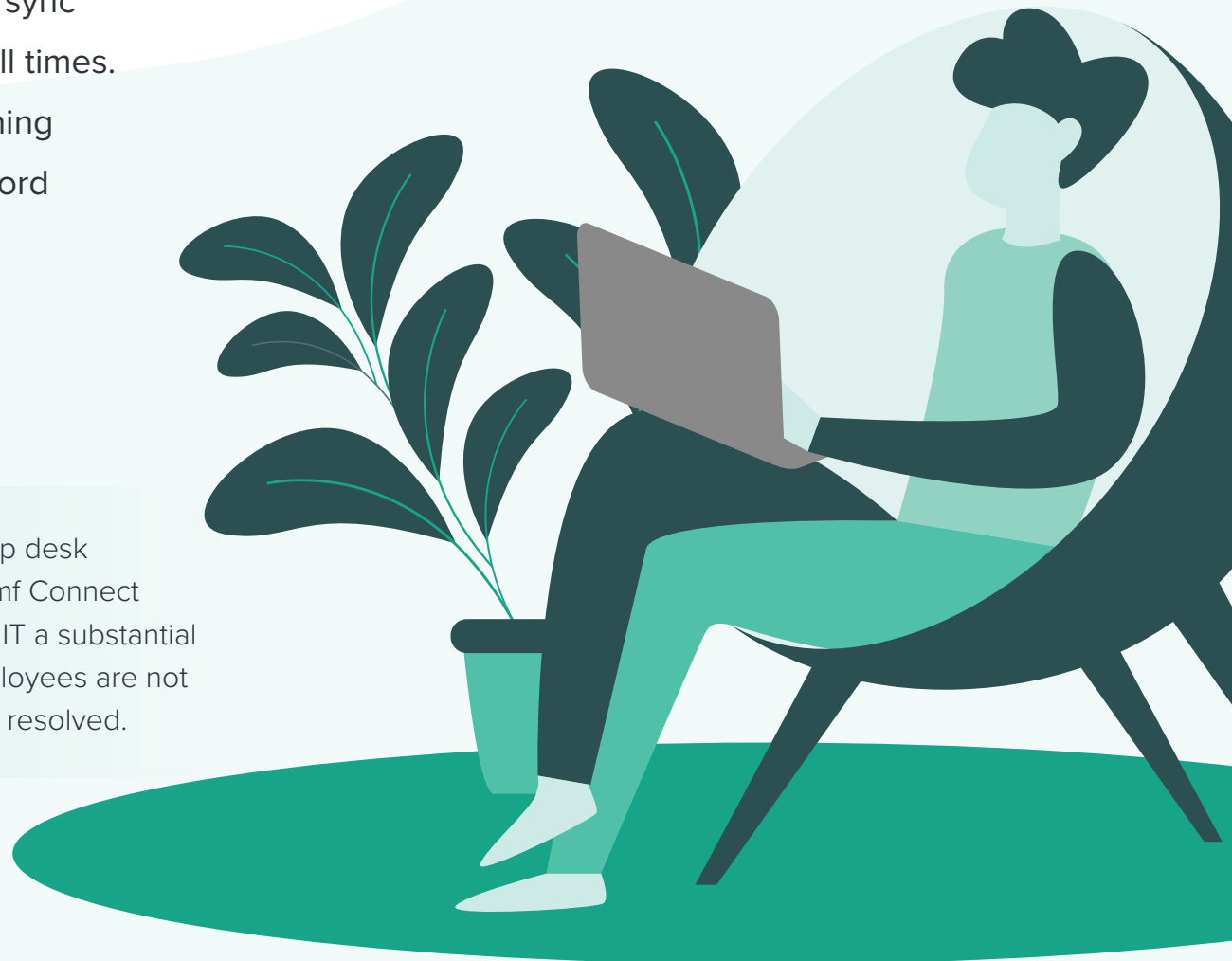
IT is able to maintain security and compliance standards across all devices by enforcing password policies via the cloud-identity provider permissions; adding an extra layer of security.



## User identity and device credential synchronization

Jamf Connect empowers employees to keep their corporate identity (cloud-based identity) in sync with their local Mac account password at all times. This means employees can access everything they need without having to input a password multiple times.

**40%** Gartner reports that 40% of all help desk calls are for password resets<sup>3</sup>. Jamf Connect eliminates these requests, saving IT a substantial amount of time and ensuring employees are not unproductive while the issue gets resolved.



# Ongoing support for remote employees

Onboarding and instant, secure connection to resources are the first two steps in promoting a productive remote workforce. But, just as important is the ongoing management of the device.

**Jamf Pro** and **Jamf Now** communicate with devices through **Apple's Push Notification service (APNs)** and tell them how to behave. This maintains a constant connection to devices, so IT doesn't have to.

When IT wants to modify a device (remote or on-site), they simply send a configuration profile or management command via APNs. VPN, email, Wi-Fi and countless more settings can automatically be applied to an employee's device — without requiring any interaction from them.



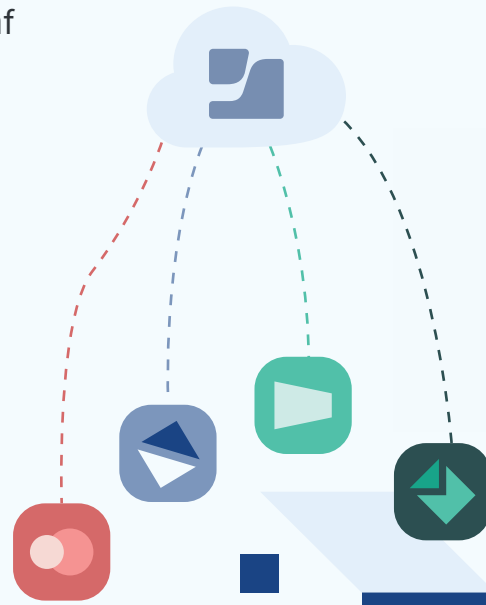
### Target devices in bulk

Intelligently target a device or group of devices with Jamf Pro's patented **Smart Groups** technology. Leverage smart targeting within Jamf Pro to collect inventory details of all managed devices and then automatically trigger action on the entire group or subset when needed. For instance, if more of your workforce is working remote, you can put them all in a Smart Group and automatically deploy a VPN configuration profile to every device for seamless access to company resources.

Or, make items available on demand to employees via [Self Service](#). IT populates Self Service with approved configurations, resources, scripts for troubleshooting common issues, bookmarks and trusted apps so employees can access and download on their own.



Day or night, in all corners of the world, users are empowered all without IT needing to answer a help desk ticket.



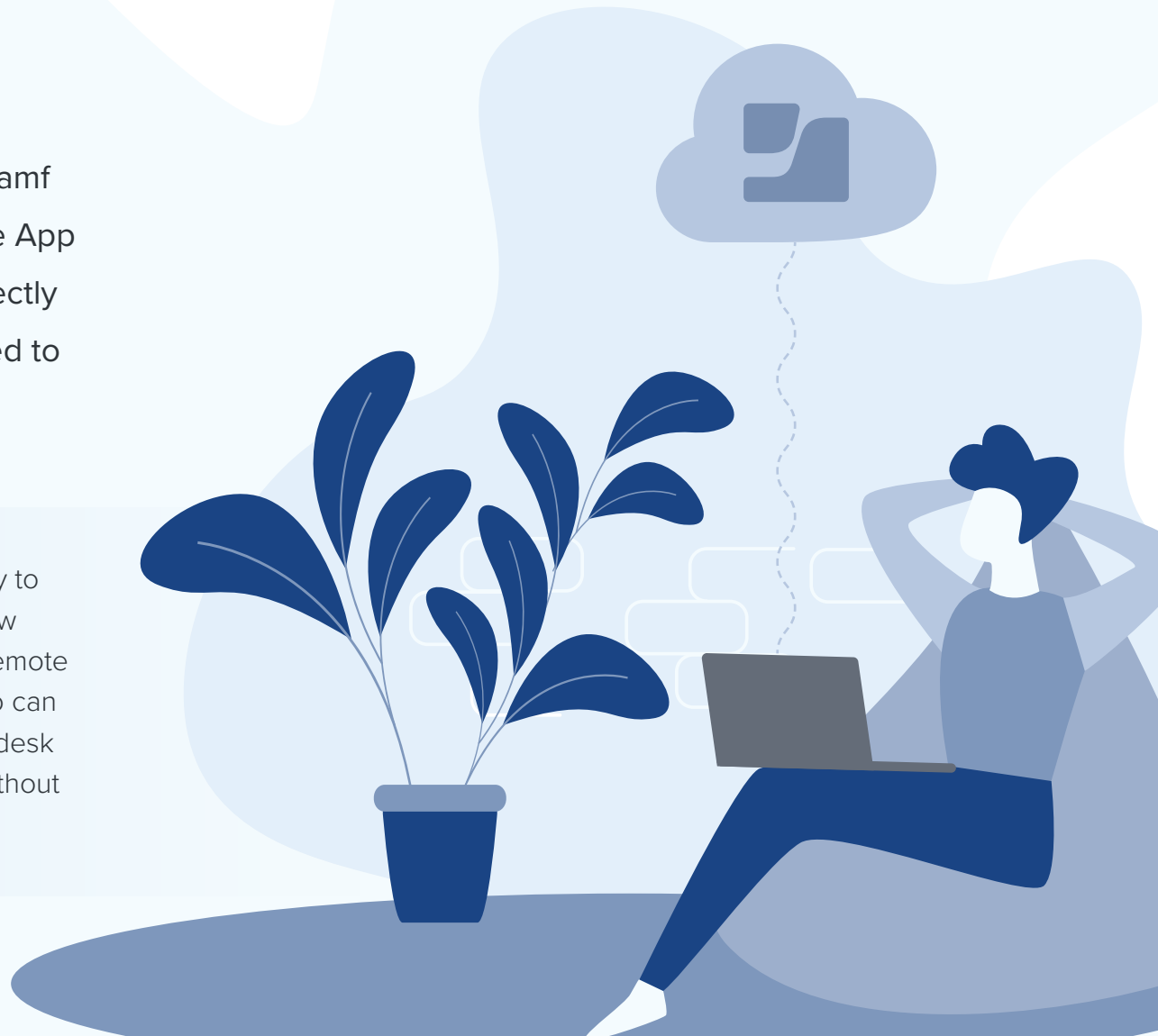
### Sophisticated app management

The business world runs on apps, so an organization's management strategy needs to adequately accommodate. Through the integration with Apple Business Manager, Jamf Pro can purchase and deploy apps from the App Store (or your company's app directory) directly to devices. Again, these apps can be pushed to devices or made available via Self Service.



Even delay operating system availability to give the IT team time to validate the new OSs before making them available to remote end users. This is another way Jamf Pro can help reduce the burden on the IT help desk and empower end users to succeed without needing IT support.

Deploying the most up to date apps and operating systems (OSs) is also important to the security of the device and organization. Jamf Pro and Jamf Now allow IT to deploy apps and OSs efficiently and monitor the process through inventory reporting.



### Better Mac protection

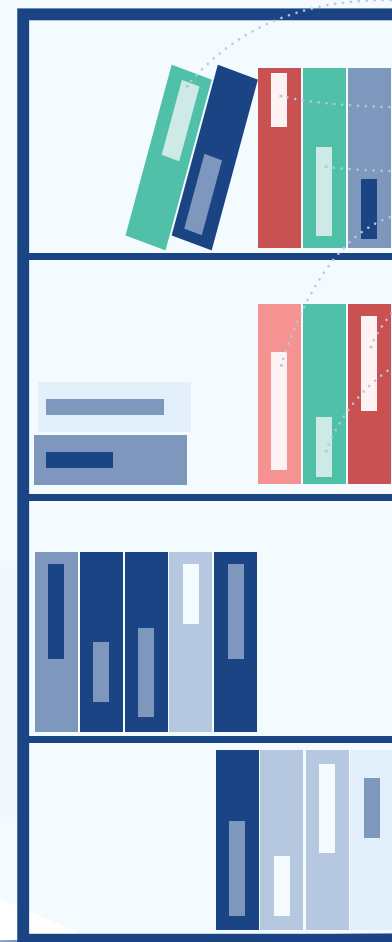
As more employees leverage Mac to do their jobs, the need for purpose-built Mac security amplifies. With employees using their computers at home, there's a whole new risk of attacks against company assets. Employees may become more comfortable visiting websites they may not normally do on a company network, personal email on devices, or trusting their child to play a game on a website. And when that inevitable piece of malware finds its way onto a device, security teams and IT face the additional challenge to remediate that attack remotely.



Jamf gives you the power to secure your remote macOS endpoints all without impacting the device experience or privacy of the employee.

By leveraging native security tools — like Apple's new Endpoint Security framework and on-device analysis of macOS system events — **Jamf Protect** creates customized telemetry and detections that give enterprise security teams unprecedented visibility into their macOS fleet, no matter where the devices are.

With Jamf Protect and Jamf Pro, you have some of the best tools available to identify and remediate incidents on macOS without the devices ever touching the corporate network:



- Receive real-time alerts of malicious activity
- Investigate activity on devices
- Set up proactive blocks for known bad applications
- Isolate a device from sensitive resources
- Eradicate malicious files on the device
- Redeploy macOS and installed applications



# Empower the modern, mobile workforce

The recent health crisis is only one reason why organizations need to put workflows in place to keep employees safe and productive no matter where they are.

The remote-worker trend will only continue and to maintain a positive company culture, remote employees must be empowered just like their on-site counterparts. Jamf makes this possible, all while delivering the best and most secure employee experience.

Get ahead of the mass-migration to home offices by starting your Jamf trial today. And once a customer, take advantage of over [130 free online training modules](#) on how to best leverage Jamf to empower your workforce.

[Request Trial](#)

Or contact your preferred reseller of Apple devices  
to take Jamf for a free test drive.

1 <https://www.talentlms.com/blog/remote-work-statistics-survey/>

2 <https://b2b-assets.glassdoor.com/the-true-cost-of-a-bad-hire.pdf>

3 <https://342sv54cwflw32bxz36tm0bv-wpengine.netdna-ssl.com/wp-content/uploads/2015/05/AD-Password-reset-tool.pdf>