jamf

Work Anywhere Checklist

The pillars of a mobile Apple-focused workforce

Jamf, OneLogin, and BetterCloud

jamf PRO
onelogin
BetterCloud

Want to modernize your organization's infrastructures for remote work? Pay close attention to identity, device and SaaS application management. Using these tools, organizations can build deployments that scale properly with the pace of business.

Due to the fundamental nature of these platforms, it is important to start off on the right foot and follow best practices. Here are tips from three industry leaders to start your mobile transformation the right way.

jamf | PRO

Device management with Jamf Pro

The user experience is where the rubber meets the road. From the first to the last day — and every hardware upgrade in-between — the device an employee uses matters.

Research has shown that employees prefer Apple devices for their reliability, ease of use and familiarity. Administrators find the management of these devices refreshingly modern when paired with Jamf Pro device management.

Device Management Best Practices

Use Apple Business Manager

Apple's free deployment programs that power device management are provided through Apple Business Manager. Start the process at business.apple.com as it can take several days for new account verification. Once you are registered, your business can seamlessly manage your devices and apps by integrating Apple's deployment programs with Jamf Pro.

Plan your enrollment

With a little prep work, Mac admins can ship devices directly from Apple or eligible resellers to employees. Jamf offers enrollment methods to ensure devices go under management remotely. Zero-touch deployment is the holy grail of Apple rollouts and it's easier to start implementing than most people think.

Embrace tier-zero support

Users of Apple devices are self-sufficient and embrace tier-zero support options. Jamf's Self Service application allows users to install their own applications and support functions without needing admin access. Users automatically have what they need, as well as quick access to what they might want.

onelogin

Identity Management

A user's identity is a powerful tool to manage and enhance their digital workspace experience. From provisioning new users to managing and auditing access to corporate applications, identity management is often the backbone of enterprise deployments. OneLogin offers complete identity and access management solutions to manage digital identities for all your workforce and customers.

Identity Management Best Practices

Provide easy access to corporate applications from anywhere

One of the most important elements of a work-anywhere model is providing employees with the right access to all the applications they need to do their work. Keeping track of numerous passwords is cumbersome for end users and password-reset requests can quickly overwhelm your IT helpdesk. Start by rolling out Single Sign-On (SSO), so users can log into a simple dashboard and launch their work applications securely with an audit trail. Layer on self-service capabilities like advanced self-service password reset to make it even easier for users to manage their own credentials and accounts.

Implement access security policies and controls for critical apps

Remote users can access confidential information and corporate applications from spaces that you don't control, such as WiFi connections you can't secure. Stay in charge without burdening users! Enable smart access policies like role-based access control (RBAC) and multi-factor authentication (MFA) immediately for critical apps, like VPN, and for privileged users — or to expand to your entire workforce. Enhance MFA with user-friendly, AI-Powered SmartFactor Authentication to further secure and enhance the login experience.

Automate user provisioning and deprovisioning

Managing a changing set of identities, user accounts, and application permissions for your workforce can be error-prone and labor intensive. Centralize visibility and management from a unified cloud directory. Automate user account provisioning and deprovisioning within your onboarding and offboarding processes to eliminate manual processes, reduce burden and cost of lifecycle management, and seamlessly prevent lingering or unauthorized access.

BetterCloud

SaaS Management

As companies grow and adopt more SaaS applications, it can become increasingly difficult to know what applications your employees are using, let alone to manage and secure them. BetterCloud helps IT and security teams deliver automated operations, resulting in reduced friction, improved collaboration and better employee experience.

Best Practices for SaaS App Management

Discover what applications your employees are using

Easily discover and analyze all SaaS applications used in your environment through OAuth and SSO detection to identify applications, users, redundancies and potential risks. You can also save money on unused licenses by monitoring app usage.

Automate formerly manual IT processes

Automate and centralize application settings and controls for fully-automated onboarding, offboarding and mid-lifecycle user changes across your environment. BetterCloud's workflow capabilities can save time, reduce human error and create a consistent experience.

Secure your data

Receive alerts on SaaS security threats and vulnerabilities in real time and automate remediation for swift, secure user interactions. Use content scanning and file-sharing policies to secure your corporate data.

Give time back to IT and control to end users. Jamf, BetterCloud and OneLogin can provide a seamless and secure infrastructure for remote and on-site employees on Apple devices.

Start your path towards modern infrastructure with leaders in device, identity and SaaS application management.

jamf

Learn more:

jamf.com/workanywhere