jamf

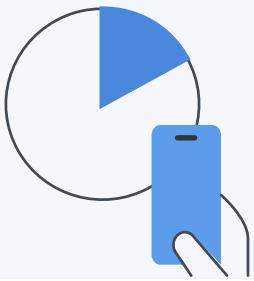
# Jamf mobile BYOD: **secure, private, simple.**


Jamf's recent **Security 360** report found that "in 2022, **21% of employees** were **using devices** that were misconfigured, exposing them to **risk**."

When devices access work resources, they need to be set up for success.

## Employees use mobile regardless

**17%** of employees **use their personal devices** for work — without telling IT.



SOURCE: ZIPPIA

## BYOD must be usable, secure and private.

If you configure and secure the work portion of devices, and allow for seamless use of work and personal apps, employees are more likely to use them. It's important to make clear that these devices must have the same level of personal privacy as those not enrolled in a BYOD program. With Jamf, admins can:

- Configure work-only settings
- Secure connections to business applications
- Build upon Apple's strong security posture
- Separate work and personal accounts to preserve end-user privacy

**Learn from Apple what MDM can and cannot do.**

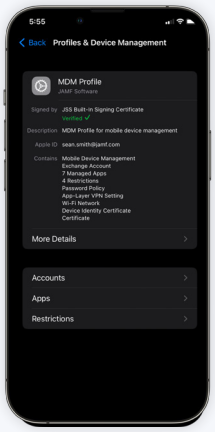
## How Jamf enables BYOD

Our solutions work together to manage and secure apps, data, and business connections, achieving **Trusted Access**. They also assure users that their privacy is intact.

### Device enrollment that protects privacy

**Jamf Pro** separates work and personal accounts with Apple's User Enrollment. This prevents organizations from seeing or controlling personal data.

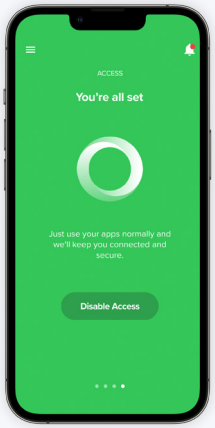
- Configure access to corporate services, including WiFi, email, and contacts
- Distribute and manage the entire library of work iOS or iPadOS apps
- Deploy data loss prevention policies, preventing data flow from managed to unmanaged apps
- Provide the native Apple experience iOS users want from enrollment to day-to-day use




### Secure access and connectivity

**Jamf Connect** ensures that only authorized users on managed devices can access work apps and data. Jamf Trust is the end user app for Jamf Connect.

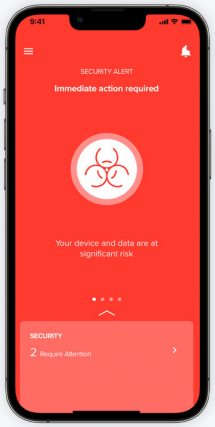
- Offer secure, encrypted connections to business applications with Zero Trust Network Access (ZTNA)
- Manage network traffic at the app level and further preserve privacy by configuring ZTNA via Per-App VPN




### Mobile endpoint protection

**Jamf Protect** enhances Apple's strong security to defend organizational data. Jamf Trust is the end user app for Jamf Protect.

- Manage app risk with workflows that vet apps to remove vulnerable or leaky applications
- Detect and intercept Man-in-the-Middle (MitM) attacks
- Perform security checks like monitoring for out-of-date or vulnerable OS versions




jamf

www.jamf.com



*Updated 2/2022.*

Find of these capabilities in one place with the Jamf Business plan. **Request a trial.**

Or reach out to your Jamf representative or preferred reseller.