Mac Management and Security Checklist for Growing IT Teams

1. Deployment and Setup

- [x] Enroll devices automatically through Apple Business Manager
- [x] Apply required configuration profiles
- [x] Use zero-touch provisioning when possible
- [x] Provide users with clear onboarding instructions

2. Configuration and Baselines

- [x] Enforce FileVault encryption
- [x] Enable Activation Lock
- [x] Apply a secure baseline configuration
- [x] Set system permissions and restrictions
- [x] Set minimum OS versions

3. Apps and OS Updates

- [x] Deploy required applications automatically
- [x] Keep apps patched and up to date
- [x] Schedule OS updates that minimize disruption
- [x] Verify update compliance across the fleets

4. Identity and Access

- [x] Integrate Macs with your cloud identity provider
- [x] Require strong authentication for users
- [x] Apply context-aware access controls
- [x] Align access levels with user roles

5. Endpoint Security

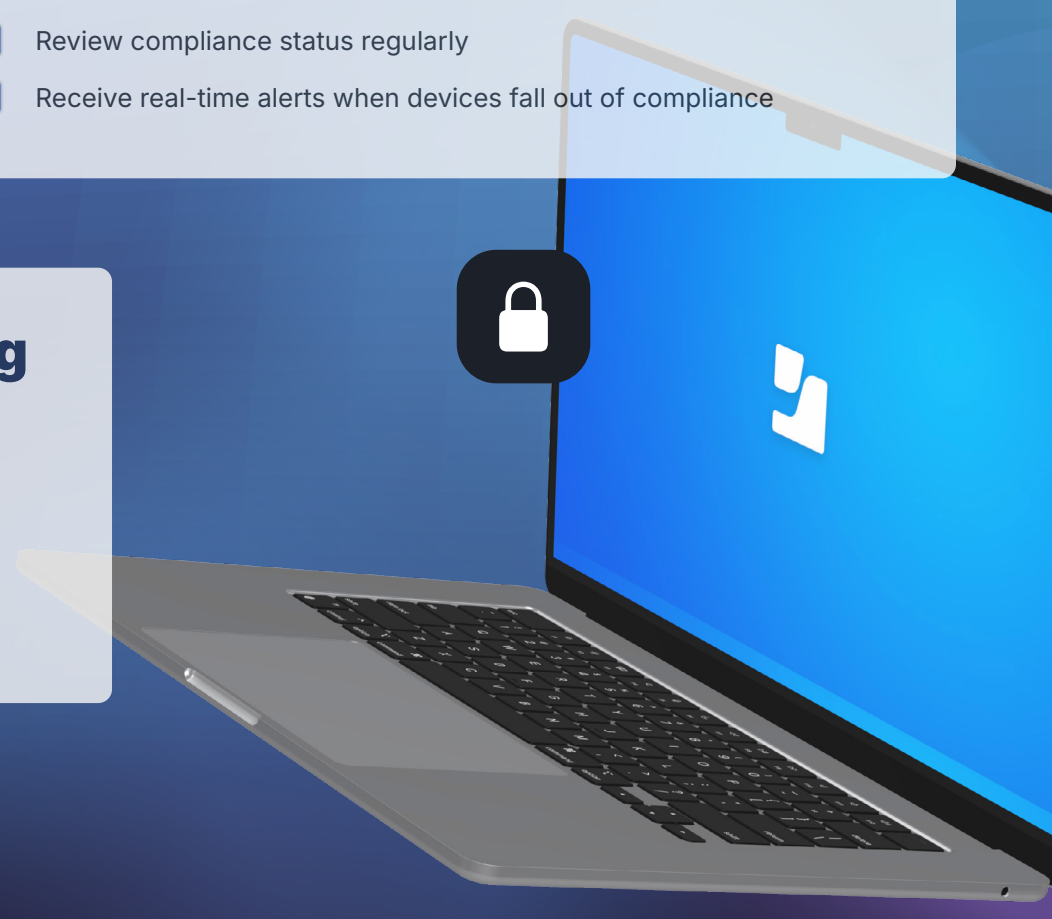
- [x] Enable AI and ML threat prevention
- [x] Use on-device detection and blocking
- [x] Monitor risky activity on endpoints
- [x] Respond quickly to incidents
- [x] Limit access to sensitive resources

6. Compliance and Monitoring

- [x] Benchmark devices against your preferred standard
- [x] Use automated workflows to enforce policies
- [x] Review compliance status regularly
- [x] Receive real-time alerts when devices fall out of compliance

7. User Awareness and Training

- [x] Train users to recognize phishing
- [x] Promote secure behavior and hygiene
- [x] Encourage quick reporting of suspicious activity
- [x] Reinforce training during onboarding



This checklist identifies essential management and security requirements.

To learn how to implement them consistently across the Mac lifecycle, download the complete Mac Management and Security Guide for Business.

Download

jamf

www.jamf.com