jamf

Is your mobile security built to go beyond MDM?

Check every statement that applies, then count your total below.

1.

THREAT DEFENSE

Mobile threats don't stop at device enrollment.

- [ ] We rely on MDM to protect mobile devices without additional mobile threat defense.
- [ ] If a user taps a phishing link on an iPhone or iPad, we have limited ability to detect or respond automatically.
- [ ] We can't easily identify apps that increase security risk on managed devices.
- [ ] We have limited visibility into or protection against unsafe Wi-Fi or other network-based mobile threats.

2.

COMPLIANCE AND DEVICE HEALTH

You can't fix what you can't continuously see.

- [ ] We don't have a real-time view of which mobile devices are currently compliant.
- [ ] Configuration drift is difficult to identify before it affects users or compliance.
- [ ] We usually discover mobile device issues after users report them.
- [ ] We can't consistently enforce OS and app version requirements across all mobile devices.

3.

UPDATES & VULNERABILITY MANAGEMENT

Every delayed update creates unnecessary risk.

- [ ] We can't guarantee all mobile devices stay current with OS updates.
- [ ] Critical app updates still depend on users installing them.
- [ ] Update deadlines aren't consistently enforced across our mobile fleet.
- [ ] Devices occasionally fall out of compliance because updates aren't applied on time.

4.

IDENTITY & ACCESS

Identity is only part of the security picture.

- [ ] Our identity platform doesn't evaluate the security posture of mobile devices during authentication.
- [ ] A compromised or non-compliant mobile device could still access business applications.
- [ ] Access policies assume enrolled devices are trusted, regardless of their current security state.
- [ ] We don't automatically restrict access from risky or non-compliant mobile devices.

Why these questions matter

Mobile device management is an essential foundation, but modern mobile security requires more than device configuration alone. Threat protection, continuous compliance, timely updates and identity-aware access all work together to reduce risk.

The more statements you checked, the more likely your environment has security gaps that device management alone can't address.

Your result

0-4 → **Strong foundation**

Your mobile security strategy is covering many of the capabilities modern IT teams need. The paper can help validate your approach and highlight additional opportunities to strengthen your environment.

5-9 → **Opportunities to strengthen**

Your environment has several common security gaps that can increase operational risk over time. Many organizations reach this stage as they scale their mobile environment. Learn how to strengthen protection without adding unnecessary complexity.

10-16 → **Time to modernize your approach**

Device management is carrying more responsibility than it was designed for. Expanding your approach to include threat defense, continuous compliance and identity-aware access can help reduce risk while simplifying operations. The paper provides a practical roadmap for modernizing your mobile security approach.

Ready to go beyond MDM?

Discover how to combine mobile management, threat defense and compliance into a modern security strategy for iPhone and iPad.

Get the paper

jamf

www.jamf.com