Evolve Beyond BYOD Framework for Mobility Management

What was once a balance between productivity and convenience is now ***a growing vulnerability.***

Why BYOD Raises the Stakes

Data Leakage

Employees may feed sensitive information into consumer-grade tools with weak privacy protections that bypass enterprise mobility security standards.

Disconnected Device Lifecycle

Discontinuity from device procurement, onboarding, support, retirement, and replacement that leaves IT teams guessing what is in use and what is decommissioned.

Fractured Cost Management

Each employee submitting a monthly expense report for data plans prevents executive insight into line-level invoice data trends and usage patterns.

Limited Mobility Optimization

Mobility data plans spread across individual workers means invoice auditing, disputes and corporate-specific plan savings are left to the end-users or not done at all.

The Mobility Evolution: COPE Frameworks

By controlling the device while still allowing personal usage, **COPE (Corporate-Owned Personally-Enabled)** strikes the right balance between enterprise mobile security and user flexibility.

Superior Security & Management

Devices can be preconfigured with mobility management and security solutions, ensuring policies are enforced.

Better Governance & Visibility

Teams gain insight into app usage, data flow, and cost anomalies without spying on personal behavior.



Stronger Compliance & Policy Adoption

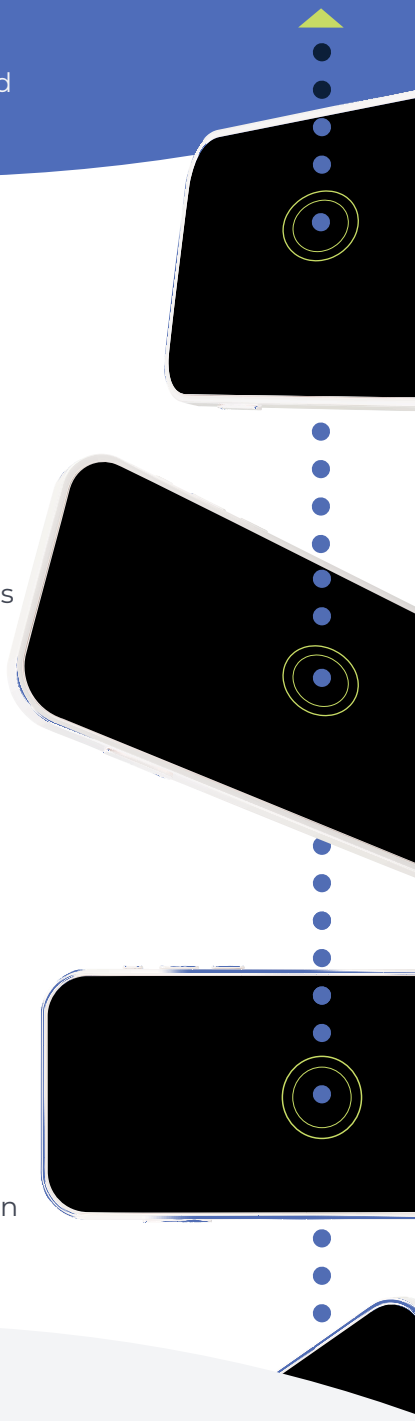
Organizations can enforce device policies employees often ignore, such as downloading unapproved apps.

Faster Support & Action

When devices are standardized and secured, organizations can support teams without worrying about local risks.

Plan Your Pivot Away from BYOD

You don't need to rip and replace overnight. Instead, think of it as a staged shift toward **secure enterprise mobility management.**



1 Audit Your Current Environment

- Identify how many personal devices access enterprise systems
- Map the apps already in use
- Quantify exposure with a telecom audit for mobile spend and compliance

2 Adopt Enterprise Mobility Management Tools

- Leverage mobility management platforms to enforce secure configurations
- Automate updates, patching, and remote wipe capabilities
- Centralize visibility across your mobile fleet

3 Establish Clear Device Governance Policies

- Define acceptable use for enterprise data on devices
- Communicate risks tied to consumer-driven and AI-enabled mobile apps
- Use policy to prepare employees for an eventual COPE shift

4 Transition to COPE Devices

- Start with high-risk groups in your organization
- Provide company-owned devices with personal allowances to ease adoption
- Highlight security as a benefit, not a burden

Your Mobility North Star for Better Outcomes with Less Effort

People once framed BYOD policies as a sign of agility. Today, it's increasingly a sign of risk where mobility security isn't optional.

Policies are the backbone of protecting sensitive data, ensuring compliance, and enabling true enterprise mobility without fear of breach or uncertainty of cost.

Start the Transition Today →

© 2026 Calero | www.calero.com | +1 (866) 769-5992