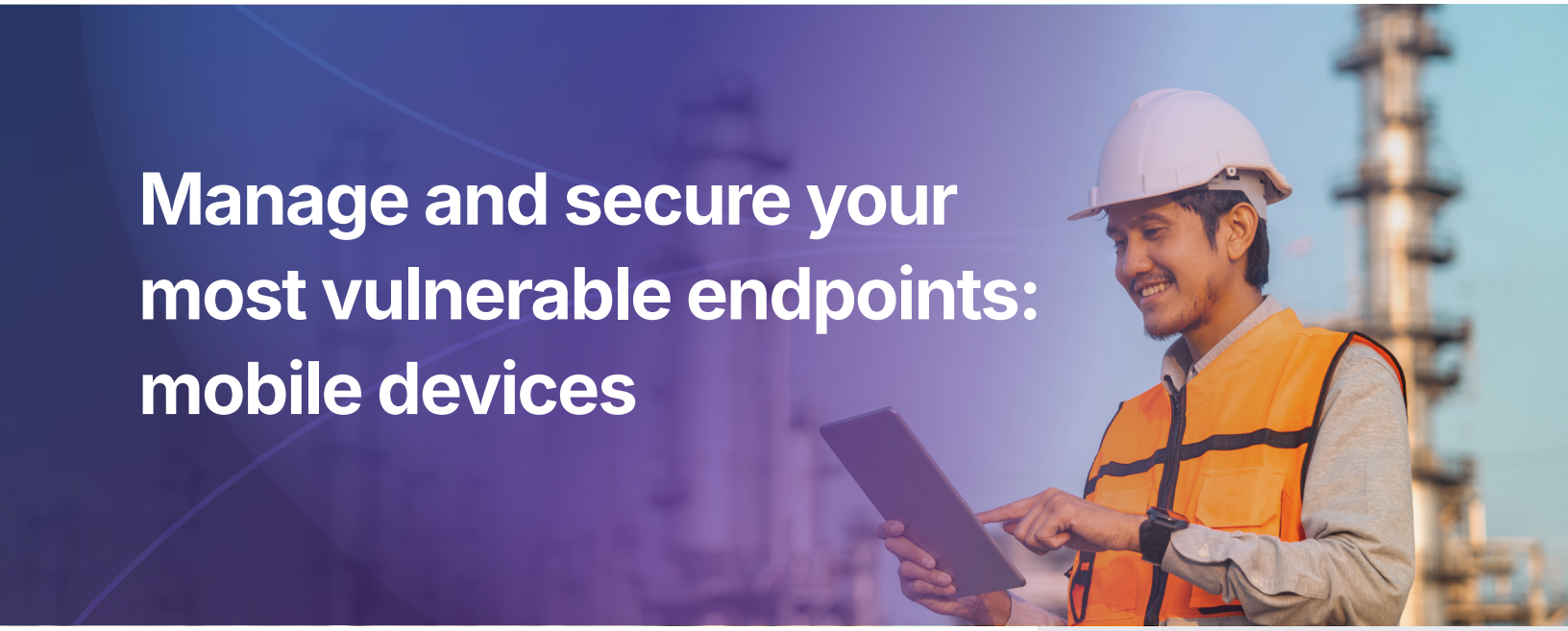
jamf

Manage and secure your most vulnerable endpoints: mobile devices



When we talk about mobile devices, we think of laptops, tablets and smartphones. While each device falls into the mobile category, this paper focuses on smartphones and tablets. Millions of users worldwide rely on these devices to accomplish their daily work, school and personal tasks. However, this dependence on mobile devices has also raised significant concerns regarding mobile security.

Keeping your mobile endpoints secured while maintaining compliance, and providing memorable user experiences is possible. After reading this, you'll know how to effectively and efficiently align mobile device protection to the same standards as the rest of your fleet.

State of mobile security

Mobile devices enable organizations to streamline operations across various business functions. With their ease of use, portability, and ability to access apps and resources from anywhere, they help both frontline and corporate teams stay connected and productive.

Dive in to learn about:

Organizations often support a range of mobile device ownership models, such as shared or one-to-one deployments for frontline workers (e.g., nurses or retail associates), and corporate-owned, personally-enabled (COPE) or bring-your-own-device (BYOD) programs for corporate staff. IT teams responsible for deployment and management must apply tailored security configurations based on each model's unique requirements. Regardless of whether devices are shared and tightly controlled or personally owned and governed by privacy considerations, it is essential to also enhance the overall user experience.

The increased adoption and dependence on mobile devices means there are greater security implications. Some of the more common ones impacting the enterprise are:

- Additional risks of data leaks
- Unauthorized access to private user information
- Lack of parity between mobile devices and the user experience
- Implementing and mantaining compliance

The gaps between the security policies designed to protect computers and the efficacy of enforcing them on mobile devices can weaken the security posture of mobile devices and may decrease the security posture of the organization overall. Another consideration is the complexity introduced when supporting multiple platforms, which impacts the speed of mobile deployments – both provisioning company-owned devices to users and ensuring that company data stays secure on personal devices used for work. All this without impacting user privacy or the usability of their device.

Another crucial consideration is whether your organization has policies that restrict mobile device usage that aren't covered under a BYOD program. If you believe your organization is immune to mobile threats, it's essential to reconsider. Start by asking yourself, do we allow personal mobile device usage?

Devices can contain sensitive data or are required to conduct essential business workflows. For example, mobile devices used by directors or VPs for normal business functions. These device are often employed for organizational communications, but also serve as more attactive vectors for attack. Or consider devices deployed for specific use-cases, like iPads for salespeople in the field or in a manufacturing floor. These devices are "out in the field", but also have specific requirements – for compliance and usability.

Mobility drivers

The conventional concept of enterprise mobility, which pertains to the evolution of how we work, has faced significant challenges that necessitated a swift shift in organizational models. This transformation was driven by various factors, including:

- The migration of operations to cloud services
- The adoption of distributed workforce patterns
- The increasing prevalence of native mobile applications

The development and use of mobile business apps seamlessly aligns with ever-changing work environments, establishing mobile devices as indispensable tools. This is primarily due to their convenience, adaptability, engagement and cost-effectiveness.

The focus here is on the significance of mobile devices and business applications in the modern, global workplace:

Mobile Devices for Work Efficiency:
Mobile devices are essential for accessing business apps and networks anywhere, enabling smarter, more efficient work.

Popularity of Mobile Apps:
Mobile devices support critical workflows and hold sensitive data, making them prime targets for attacks. Devices used by executives or field teams must balance usability with compliance.

Versatile Workflows:
Mobile devices enable efficient workflows, allowing users to video conference, message, manage inventory, access customer info, edit documents, and handle emails on the go.

Expectation of Mobile Performance:
With many users relying on mobile devices alongside or instead of desktops, there's a growing expectation for mobile tech to function seamlessly and efficiently as an extension of their work.

Workplace Innovation:
Mobile devices drive workplace innovation by boosting employee satisfaction, productivity, and retention, while helping organizations work more efficiently and adapt to change.

Continued Growth of Mobile:
Mobile devices dominate internet and work-related usage, with a 62.22% global market share in 2024—far surpassing desktops and tablets, according to Statcounter GlobalStats.

Remote and Hybrid Work Environments:
Mobile adoption remains crucial for enabling remote and hybrid work, with 95% of employees favoring remote options. Mobile devices drive collaboration and flexibility, regardless of physical location.

Global Mobile Device Penetration:
As of 2024, 7.4 billion people worldwide own mobile phones, with smartphones making up 71%—about 6.7 billion subscriptions—highlighting the global scale of mobile adoption.

The mobile enterprise deployment landscape

In the past, organizations typically made a deliberate choice to align their business needs with a single platform, often centered around Microsoft Windows. This involved procuring computers that were compatible with the chosen operating system (OS). Through enterprise agreements with Microsoft, organizations could delay the deployment of the latest Windows version until they were prepared for the transition. The advantage was that older OS versions received continued support for an extended period to accommodate the needs of these organizations.

However, here lies the challenge: the mobile landscape, historically considered a consumer-oriented arena, approached OS patches as updates that should be implemented as soon as they become available. With users controlling when updates occur and how quickly after release they are installed, enterprise usage has seen this as an obstacle to adoption due to the:

- Diverse array of mobile OS options
- Fragmentation among supported versions within each OS
- Evolving deployment methods across various OS types
- Disparate support leading to delayed upgrades
- Variable support for business apps among OS versions
- Differing update schedules and feature support by developers
- Different ownership models impacting management (e.g., BYOD vs. COPE)
- Supported vs. unsupported features in MDM solutions (native vs. non-native for frameworks)
- Varying security levels across OS types
- Limited policy-based enforcement for compliance requirements

Rising concerns

We've touched on security concerns related to the rapid growth of mobile device usage in organizations. In this section, we'll delve deeper into the threats targeting mobile devices and the risks associated with their use. We'll also address common misconceptions about securing mobile devices in the workplace.

The first issue arises from the mobile nature of these devices, which are appealing targets for threat actors for several reasons:

Valuable Data Storage:
Mobile devices contain a wealth of personal, business and regulated privacy data, like PHI (personal health information) — even non-regulated but sensitive data like PII (personally-identifiable information). Threat actors can exploit this information for various purposes, potentially launching attacks on users or organizations. It's crucial to safeguard this data through multiple layers of protection to ensure that only authorized users have access.

Susceptible to Loss or Theft:
Mobile devices' portability allows users to work from various locations but also increases the risk of theft or misplacement. Threat actors can seize opportunities to steal devices, posing a direct threat to data security. Even a brief moment of unattended access to a device can compromise it or make it susceptible to future attacks.

Misconceptions About Security:
Some believe more than diverse security solutions are required. However, the rapidly evolving mobile threat landscape demands native support for endpoint frameworks. Relying on solutions that lack this support may increase vulnerability by leaving open attack vectors in unsupported functions and features.

Over-protected or under-managed: finding the balance

Balancing device management with security is a critical concept in the context of optimizing mobile technology to support frontline workers. While it may seem like a conflict between IT and security priorities, the reality is that focusing solely on either management or security is insufficient. Organizations must integrate both elements seamlessly to create a mobile security solution that supports efficiency and effectiveness.

The challenge is finding the right equilibrium. Excessively locking down devices with rigid security measures can hinder user experience, reducing frontline workers' productivity. On the other hand, neglecting security puts valuable data and operations at risk. The key is not to choose between security and productivity but to align both, ensuring mobile management and security work together to support frontline teams while safeguarding organizational assets.

Issues	Over-protect	Under-manage
Compromised performance		✓
Usability		✓
Shadow IT (privacy concerns may drive employees to use personal devices)		✓
Bypassing corporate security measures		✓
Undermines mobile workspace potential		✓
Compliance with regulatory requirements	✓	
Mitigates evolving mobile threats	✓	
Segments business data in a separate, encrypted volume from personal data	✓	
Ensure patch mitigation occurs at a regular cadence	✓	
Streamlines deployment of mobile endpoints	✓	
Prevents unauthorized access to company resources	✓	
Adequately preserves user privacy while protecting business resources		✓

Here are some strategies that can help organizations transition toward a mobile security approach that prioritizes user privacy while enhancing security measures:

1. Prioritize User-Friendly Security Workflows: Integrate ease of use and simplicity into security processes. This benefits users and the teams responsible for managing and securing mobile devices.

2. Shift to Data-Centric Security:
Instead of solely focusing on device security, adopt a data security mindset. While protecting devices is important, they are replaceable. Sensitive data, on the other hand, must always be safeguarded.

3. Embrace Diverse Ownership Models:
Be open to different ownership models and tailor security measures to protect company resources accessible from various user devices. Ignoring certain devices create vulnerabilities in your overall security strategy.

4. Comprehensive Data Protection:
Ensure data is secure in all its forms. This involves encrypting volumes, keeping business data separate from personal data and securing data transmitted over any network connection.

5. Adopt Modern Mobile Technologies:
Embrace technologies designed to meet the requirements of contemporary mobile devices. Legacy security tools often fail to defend against emerging mobile threats, offering partial and not comprehensive security protections.

6. Implement Split-Tunneling:
Recognize that mobile efficiency is vital. Route business data that requires protection securely while allowing non-business data, like personal information, to bypass company security protocols. This split-tunneling approach maintains data security while respecting user privacy on BYO devices.

Outcomes of treating mobile like computers

What implications does the increasing integration between macOS and iOS hold for the future of mobile and endpoint security?

While comparing Mac, a desktop OS, to mobile devices might seem like comparing apples to oranges, the fact remains that each new iteration of macOS and iOS brings greater levels of convergence between these operating systems. With each release, the question about the significance of this integration becomes increasingly relevant.

However, the more critical inquiry is how organizations can leverage this deeper integration. Here are some ways in which this integration extends across various device types:

- Swift security gap remediation
- Seamless return to productivity
- Improved employee experience
- Establishing employee trust
- Infrastructure-wide compliance enforcement
- Deeper alignment with organizational policies
- Comprehensive, layered security processes
- Bilateral app management
- Defense-in-depth strategy, regardless of ownership model
- Flexible yet robust security and management solutions that work together for comprehensive support

Mobile compliance

Compliance isn't exclusive to regulated industries. While it's essential for organizations in sectors like finance, healthcare and education, it also encompasses adhering to rules and policies established within an organization to meet its unique business needs while minimizing risks to business continuity. In light of this, implementing and enforcing an organization-wide mobile policy, akin to how you handle Mac devices today, plays a central role in establishing a comprehensive mobile security strategy across your device fleet.

Consider this example: Mobile devices face heightened risks of theft, loss or compromise in hybrid and remote work scenarios, potentially jeopardizing sensitive corporate data. IT can enforce encryption standards and secure authentication protocols for devices and users by utilizing a MDM workflow to deploy standardized security configurations. Moreover, remote wipe capabilities can securely erase data from affected devices when necessary.

Organizations can develop a compliance plan for mobile users, whatever its use case.

This approach addresses inherent risks while providing a solid foundation to build upon. This is particularly valuable for mitigating risks associated with emerging paradigms, **such as newly designed mobile applications versus a mature website that is** already compliant with regulations like the California Consumer Privacy Act (CCPA).

Additionally, compliance involves mitigating and identifying issues before they escalate into critical vulnerabilities or regulatory violations. Here, the combination of security (monitoring) and management (enforcement) collaborates to detect and mitigate threats, ensuring that mobile devices remain compliant.

Given the versatility of mobile devices, users may inadvertently use approved services for personal tasks or unapproved apps for business-related tasks. Both scenarios pose risks, such as data mingling, compromising user privacy, or exposing the organization to data breaches and regulatory violations.

By treating mobile compliance with the same seriousness as other endpoints, organizations can ensure all endpoints accessing corporate resources have the same level of protection against the latest threats, and maintain accurate records of device inventory, usage, issued devices, employee access to corporate data and deployed security measures.

One final consideration in mobile compliance revolves around ongoing user security training. This aspect, often overlooked but vital in a comprehensive mobile security plan, **equips users with knowledge about security best practices**, secure workflows and procedures to follow when encountering potential security threats. This training acts as a critical safeguard, complementing the management and technical security measures.

Simply put: cybersecurity is not just an IT or company responsibility – it's everyone's responsibility.

Keys to unifying mobile management and security

In case it isn't yet clear, let's make it crystal: the key to security is unifying management and security for your entire fleet.

1. Convergence:

Achieving success occurs when management and security are seamlessly integrated alongside robust security protocols within a modern, mobile-centric workspace.

2. Overcoming:

Overcoming mobile security issues requires a comprehensive solution vs. traditional piecemeal approaches where multiple tools are stacked together without any single tool proving particularly effective.

3. Consistency:

Ensuring uniformity involves measuring security baselines across devices and proactively monitoring endpoints for changes that could signify the presence of issues and whether security threats, vulnerabilities or anomalies require investigation.

4. Usability:

Prioritizing the user experience and harmonizing it with protection is integral to a comprehensive strategy, emphasizing the delicate balance between effectiveness and simplicity for IT, security teams and end users.

5. Response:

Swiftly addressing security threats is essential, with a focus on prioritization, investigation and resolution that encompasses all device types, spanning different platforms and across the entire infrastructure.

6. Balance:

Striking the proper equilibrium means achieving security without compromising the user experience, reaffirming the possibility of seamlessly merging safety and user satisfaction.

We imagine a future where every device enjoys uncompromised protection without any need for trade-offs. This vision represents the ultimate goal: balanced, comprehensive data and privacy protections extended to every device in your infrastructure.

Let Jamf help you assess your organization's security needs and how to manage and protect all of your endpoints.

jamf

www.jamf.com

Get Started

Or contact your preferred reseller to take Jamf for a free test drive.