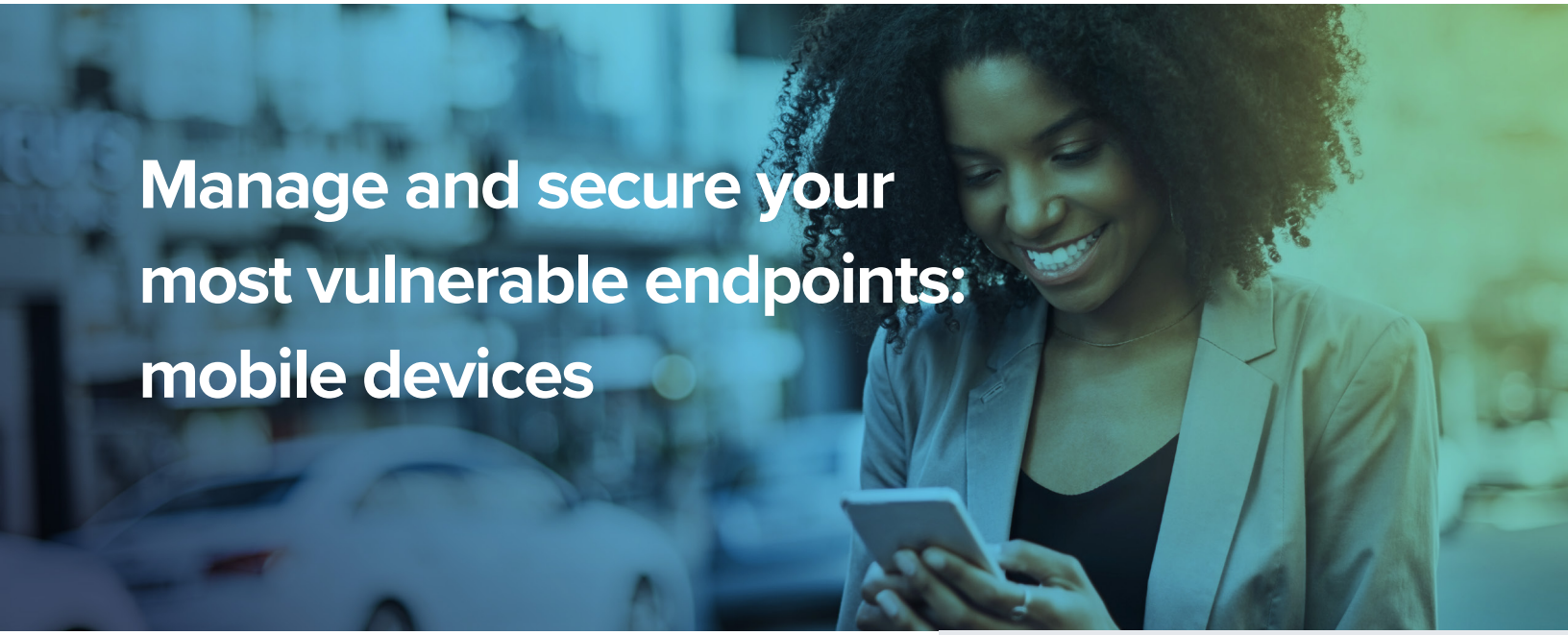
jamf



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 alongside your existing Mac fleet is possible. After reading this, you'll know how to effectively and efficiently align mobile device protection with the same best-in-breed endpoint security solution that keeps your entire fleet — Mac and mobile — safe and data secured.

Dive in to learn about:

State of mobile security

As technology advances, people are increasingly using mobile devices. These devices offer the capabilities of a desktop computer but in a slim, lightweight, energy-efficient design. They provide all-day usage, fast network connections, and access to various apps and services from anywhere, anytime.

From a business perspective, mobile devices mitigate the limitation of where work can occur while the network connectivity capability has eliminated the reliance on specific platforms, thanks in part to providing real-time access to cloud-based services. While there is a cost factor to providing company-owned mobile devices for each employee, the widespread mobile device adoption for personal use shaped multiple ownership models for organizations, like corprate-owned, personally-enrolled devices (COPE), employee choice programs and Bring Your Own Device (BYOD) initiatives. With BYOD, companies benefit from cost savings introduced by allowing users to utilize their personally owned devices for work. In contrast, users can accomplish work tasks using the platform and form factor they prefer.

But 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 Mac endpoint security
- Difficulty in assessing and maintaining compliance
- Compromise of devices can lead to data breaches

Organizations often have a false sense of security. 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?

For those organizations that answer "No," it's worth posing a follow-up question: What about scenarios like the CEO using a tablet while traveling? This tablet, which their children also use for homework, may be configured to access private company email messages. Or consider the smartphones used by board members and directors for scheduling meetings and discussing confidential business operations. These devices are often employed for organizational communication and can serve as potential vectors for attacks, including those associated with whaling campaigns.

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, such as smartphones, have become essential tools for work. They enable users to access business applications from anywhere and connect to networks, promoting smarter and more efficient work practices.

Popularity of Mobile Business Apps:

Mobile business applications are gaining popularity due to their seamless adaptation to dynamic work environments. They are considered indispensable for their convenience, personalization, engagement and cost-effectiveness.

Versatile Workflows:

Mobile devices facilitate the development of effective workflows for various work tasks. Users can easily perform activities like video conferencing calls, enterprise messaging, collaborative document editing and handling business emails on their mobile devices.

Expectation of Mobile Performance:

With many users supplementing traditional desktop computers with mobile devices, there is a growing expectation that mobile technology should work seamlessly as a natural extension of one's work capabilities, both efficiently and quickly.

Workplace Innovation:

Mobile devices play a crucial role in workplace innovation, helping ensure employee satisfaction, productivity and retention. They enable organizations to find simpler, more efficient ways of accomplishing tasks and adapting to changing work environments.

Continued Growth of Mobile:

Mobile devices continue to dominate the market, with most users accessing the internet and performing work-related tasks on mobile devices, as indicated in mobile's continued market share growth year over year, with the "worldwide split among mobile, desktop, and tablet users was 58.72%, 39.18%, and 2.1%," according to Statcounter GlobalStats.

Remote and Hybrid Work Trends: The demand for flexible workspaces, accelerated by adopting remote work solutions in 2020, aligns with the widespread use of mobile devices. Mobile adoption is a key enabler of remote and hybrid work environments, as evidenced by employees' strong preference for remote work. FlexJobs found that 97% of polled workers desired a remote work option in some capacity, be it a fully remote or hybrid model.

Global Mobile Device Ownership:

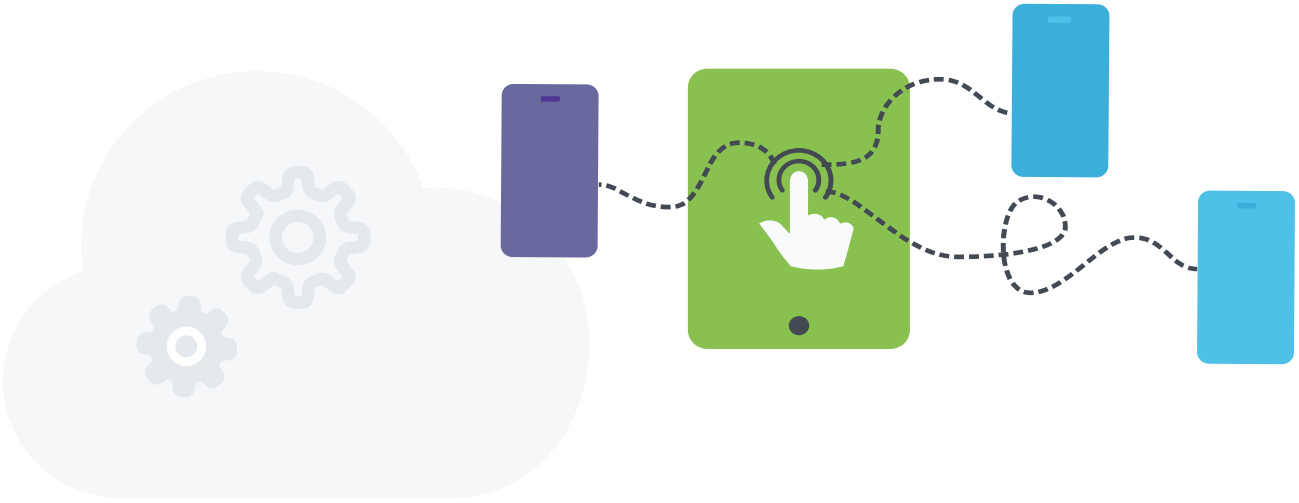
The widespread adoption of mobile devices is highlighted by the fact that a vast majority of the world's population owns mobile phones, with smartphones making up a significant portion of these devices. According to Statistica, in 2023, 90.97% of the world's population owns mobile phones with smartphones making up 85.88% of them.

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:

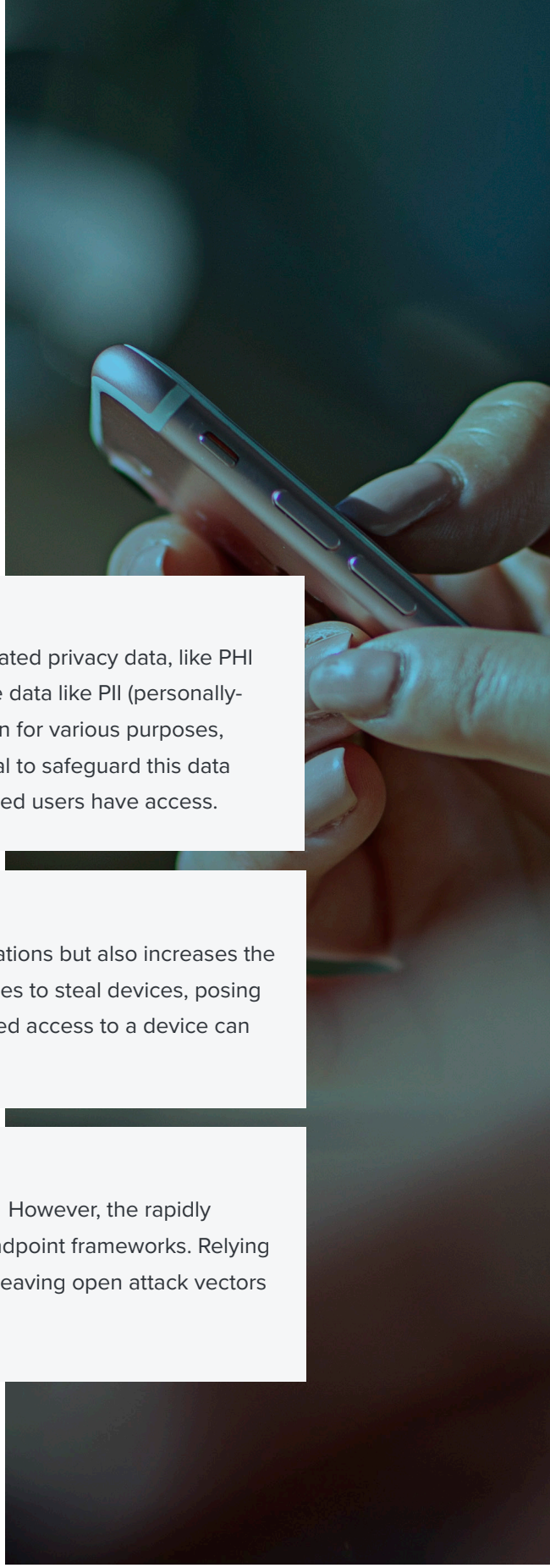
- **Diverse array of mobile OS options**
- **Fragmentation among supported versions within each OS**
- **Evolving deployment methods across various OS types**
- **Disparate support leading to delayed upgrades**
- **Variable support for business apps among OS versions**
- **Differing update schedules 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:



1

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.

2

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.

3

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

Balance is a critical concept in the context of mobile technology and the broader realm of security and management. Although it's often framed as a tug-of-war between IT and security teams, the reality is that relying solely on an MDM solution falls short. Organizations should approach management and security as integral components to establish a truly effective mobile security solution.

The challenge lies in finding the proper equilibrium. Overly securing devices through a patchwork of solutions can lead to a subpar user experience while neglecting mobile security can jeopardize valuable assets. It's not a matter of choosing one over the other but embracing the balance between management and security as the guiding principle for effective and adaptable mobile security.

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		✔

The holistic approach: lessons from the Mac paradigm

If your company secures Mac computers, why wouldn't they also secure mobile devices?

Regardless of your industry or regional location, organizations worldwide have and continue to adopt Apple devices for work. Consider that less than two years ago, according to Apple Statistics, Apple's annual revenue was $365.8 billion! The percentage of that revenue generated from iPhone (51.9%) and iPad (8.8%) combined sales was 60.7%. The Apple Watch alone sold more than iPad and Mac (9.8%) individually, accounting for 10.4% of the total revenue.

There is a clear demand for mobile devices running various operating systems, including iOS, iPadOS, Windows, Android and ChromeOS.

It's worth noting that the strategies employed to protect these underlying operating systems share more similarities than differences. This does not suggest they are identical, but some parallels can be drawn. For instance, the much-praised Apple user experience and the emphasis on the balance of security, management and privacy can be directly applied to mobile security in meaningful ways. This approach allows for a comprehensive strategy to safeguard all endpoints in your fleet from potential threats.

The basis for effective Mac security starts with Apple itself. It's rooted in how they develop their hardware and software, seamlessly integrating components with security and privacy protections woven in from the start rather than as an afterthought or separate addition. A key element that reinforces this foundation is the utilization of Apple's native frameworks. Developers must adhere to these frameworks to ensure the confidentiality, integrity and availability of data whenever users engage with their devices.

Considerable thought goes into crafting these frameworks to align with Apple's core principles, such as user-friendliness and simplicity. Interestingly, these principles also address a common criticism of security measures — that stringent security restrictions hinder users' ability to work efficiently and comfortably. Once again, it's about striking a balance.

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 can 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, leading to a false sense of security.

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 Mac:

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

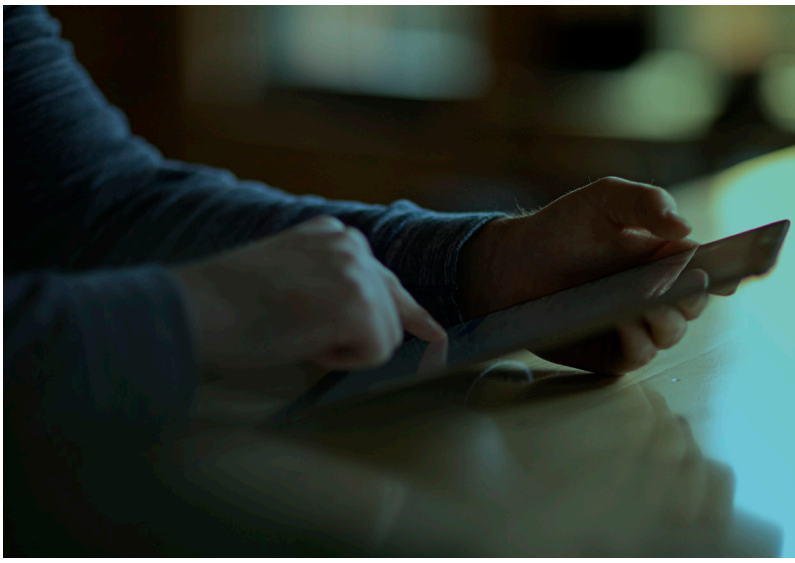
Mobile compliance

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 that builds from an existing Mac compliance plan. 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 Mac compliance, organizations can secure their mobile endpoints against the latest threats and maintaining accurate records of device inventory, usage, issued devices, employee access to corporate data and deployed security measures—just like Mac.

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 and Mac 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: enterprise-secure, consumer-simple technology that end users love and organizations trust. Our vision is seamless management and protection in every context. We call it **Trusted Access.**

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.