iManage

Making knowledge work

SECURE AND PRODUCTIVE FROM ANYWHERE

How embracing mobility empowers a modern workplace.

Introduction

After the overnight shift to remote work at the beginning of the pandemic, many people found that working outside the office suited them just fine, if not better, than the traditional setup. Many organizations have also found remote work to be a positive change—according to a study by Okta,[1] 84% of organizations consider it at least somewhat likely (44% very likely) that they will continue increased work from home capabilities going forward because of the improved productivity.

With that in mind, it's important for organizations to evaluate the setup and security of their remote and hybrid work arrangements. The majority of respondents (54%) to the Okta survey confirm that the COVID-19 pandemic accelerated migration of workflows to cloud-based apps. And with 85% of organizations embracing BYOD (Bring Your Own Device) for work,[2] a carefully considered mobility policy is also essential. Flexible work and mobile devices are here to stay —the key is embracing the benefits and minimizing the risks.

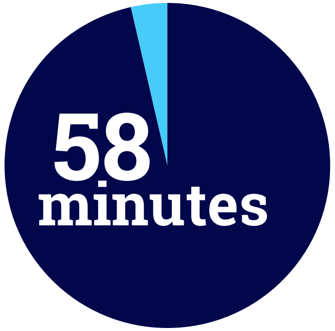
[1] https://www.okta.com/sites/default/files/pdf/2020-Remote-Workforce-Security-Report-OKTA.pdf

[2] https://www.bitglass.com/press-releases/2018-byod-report-mobile-security-threats

More productive from **anywhere**

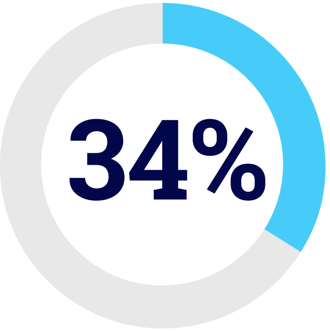
The upheaval of 2020 and beyond has made mobility — the adoption of phones, laptops, and tablets — essential for employees navigating a new way of working.

Studies show that using mobile devices for work increases productivity and saves time. One study by Samsung[3] found that:

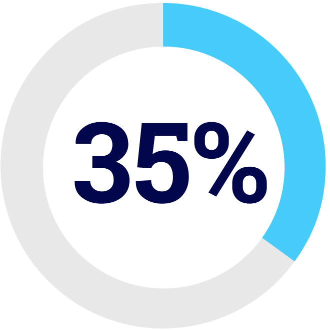


By using smartphones, workers gain **nearly an hour of work time** a day

Demonstrating an estimated increase in productivity of



The study also found that:



of respondents felt that their **output quality improved** when using a smartphone for work.

It's important to note that for the best productivity outcomes from mobile devices, you need a thoughtfully designed user experience that allows seamless interaction across the end user's workflow.

By supporting the technology within an application, you can reduce the amount of context switching between screens, applications,

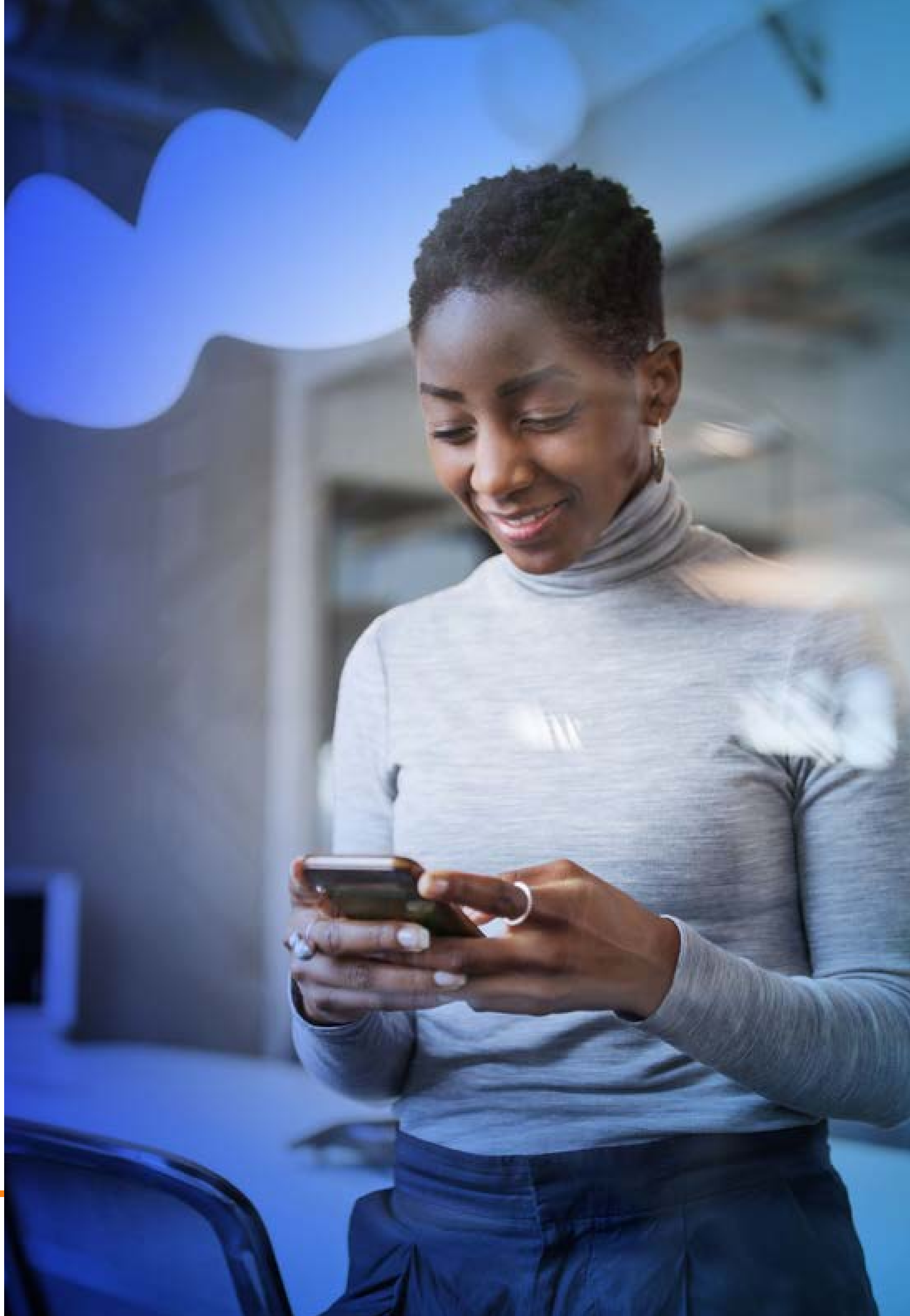
[3] https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/

and programs. Context switching has been shown to reduce productivity by 20% per context or task,[4] which across the daily activities of an entire team can add up to a lot of wasted time. The more you can make the mobile experience resemble the computer experience, the easier it is for your team to remain productive and happy on their devices.

That being said, a good mobile experience requires more than a simple lift-and-shift of features to a mobile platform. It is important to carefully consider how people work in a mobile environment and the tasks they need to perform. If your team is using these applications every day, then it is imperative that they are powerful and intuitive using functions and features that are already familiar from consumer applications.

A well-designed mobile application will also plan for online to offline transitions providing a seamless experience for users switching between environments. Whether offline in the courtroom or airplane or connected in a coffee shop, a properly designed mobile application will make it easy for users to pick up where they left off for minimal workflow disruption.

[4] https://blog.rescuetime.com/context-switching/



Keeping data secure, **everywhere**

Highly regulated functions that manage large volumes of sensitive data may feel hesitant to embrace a mobility strategy over fear of confidential data being shared in the cloud or inadvertently allowing unauthorized access to content.

Security and governance are necessary considerations for any mobility strategy, but it's important that enterprises provide a secure work environment for employees to use while mobile. If they aren't given an approved, safe option to use while on the go, they may turn to third-party cloud storage systems that are convenient but may not be configured as securely as necessary. Not embracing mobility over fears of data leaks could actually create more security risks.

Whether your organization elects to provide mobile devices or allows employees to use their own, your users need a secure method for reviewing and editing documents while mobile — ideally, one that replicates the experience and security of your organization's document management system (DMS) and other business applications. It is also critical to allow your organization to manage device access requirements and compliance at scale, while protecting content and data with granular policies for data loss prevention. Your organizational data should also be kept secure in a defined container, separate from the end user's personal apps and data.

Adopting well-designed, secure mobile applications for work as well as employing industry best practices can ensure your organization gets the best results from embracing mobility.

Best-in-class **security** while on the move

iManage Work is known for industry-leading security,[5] and the mobile application is no different. The iManage Mobility App[6] enables your team to securely work on documents from anywhere and offers a user experience consistent with iManage Work 10.

With Mobility, users can effectively transition from their computer to their mobile device without sacrificing productivity—the application remembers user settings so your employees can pick up where they left off, minimizing context switching. The app also provides the same rich search capabilities as Work 10, making it easy to find documents and edit them whenever, wherever.

iManage has designed the mobile experience to be optimized for the tasks most commonly done on mobile devices. The iManage Mobility app provides iManage Work functionality on iOS devices such as iPads and iPhones. This application enables users to view, download, and edit iManage Work documents, and upload the edited copies or new versions to iManage Work. Users can also preview, reply, reply all, and forward their iManage Work emails, and download email attachments.

Mobile Device Management (MDM) is an essential security component of any company's mobility strategy. iManage Mobility is supported with all leading MDM vendors. When you deploy iManage Mobility as a managed application through an MDM solution it allows you to control and monitor enterprise access on the end users' devices as well as easily provision and govern the applications on their devices that would have access to the enterprise content, which is critical from a security and governance perspective.

[5] https://imanage.com/products/work/

[6] https://imanage.com/products/mobility/

iManage Mobility and Microsoft Intune are **better together**

The integration between iManage Mobility and Microsoft Intune extends additional security built for mobile environments. Microsoft Intune delivers unique capabilities that enable deep integration between iManage Work and Microsoft applications, while ensuring that enterprise data remains secure.

Intune allows organizations to manage device access requirements and compliance at enterprise scale, while protecting applications and data with granular policies for data loss prevention. The result is that organizational data is kept secure in a defined container, separate from the end user's personal apps and data. Intune also ensures iManage content cannot be shared with personal Microsoft365 accounts and prevents unauthorized applications from accessing iManage content, making it safe for mobile use without the risk of data leakage. Intune works in tandem with Microsoft Azure Conditional Access to enable state-of-the-art mobile access security, with comprehensive controls for managing user and device identity.

With iManage Mobility and Microsoft, your users can stay secure and productive anywhere, on any device, with identity- and intelligence-driven innovations.

Best practices for mobility deployment

To get the best outcomes from iManage Mobility, it is important to understand best practices for an optimal mobility deployment.

STEP ONE: Get cross-functional buy-in. A good cross-functional mobility policy encourages buy-in from all leadership teams, ensuring that you're making informed decisions and that every department is involved. Understanding different use cases for every part of your organization, how mobility will facilitate their everyday workflows, and how policy change impacts them can get everyone on the same page early on, so the mobility policy agreement meets everyone's needs.

STEP TWO: Choose an MDM solution. Having a robust mobile device management (MDM) solution in place is key to ensure all devices and access rights are managed efficiently and securely.

STEP THREE: Put the right security protocols in place. Mobile security requires security teams to take a new approach. Security Containerization through your MDM siloes your corporate data, protecting against malicious or accidental data leakage. It also enables your IT administrators to remotely wipe or lock devices if they're lost or stolen. Employees should also be encouraged to add multi-factor authentication to their devices and use strong passwords.

STEP FOUR: Determine device compliance standards. If your organization chooses to embrace mobility, a policy needs to be made to ensure there is a base level of protection that's provided by the employee-owned mobile device and that it has the appropriate capabilities. Even if the device can be enrolled in an MDM, the user experience can be compromised if the device is too out of date. If a device doesn't have a certain operating system or patch level, it should not be allowed to be enrolled to ensure an optimal user experience that enables the needed productivity.

STEP FIVE: Create role-dependent policies. Not all end users need to have the same level of access. Having the right level of security policies that are flexible to meet the needs of the end users will ensure they can be productive from anywhere while still meeting stringent security and governance requirements. Some roles, such as upper-level management, need different security access policies, while others may only need access to standard business applications.

STEP SIX: Provide end user education. Educating your employees about your mobility policy and potential risks can help them stop threats before they have a chance to become breaches. Employees should especially be properly trained in security risks they may face while using their devices, as well as the proper measures required to prevent and respond to these security incidents.

STEP SEVEN: Choose the right applications. With the enterprise-grade mobile security offered by iManage and Microsoft, your users are secure and protected while using the familiar applications they rely on every day.

Empower productivity **everywhere** while remaining secure

Remote, hybrid, and mobile work are here to stay. By developing a sound mobility policy, your organization can benefit from improved productivity while protecting your critical data—and, perhaps most crucially, your organization's reputation.

Learn more about how iManage Mobility can complement your mobility journey here.

iManage

Making knowledge work

Contact us:
www.imanage.com/contact-us/

Visit our website:
www.imanage.com

twitter.com/imanageinc

youtube.com/imanage

linkedin.com/company/imanage