Protecting Unmanaged Devices in the New Work-From-Home and Hybrid Work Models

The Shifting Security Landscape of a More Mobile Workforce

66% of organizations will continue with **remote work** or implement a **hybrid work model.**

51% of enterprises say their mobile workforce regularly experiences **mobile phishing** on their business-use devices.

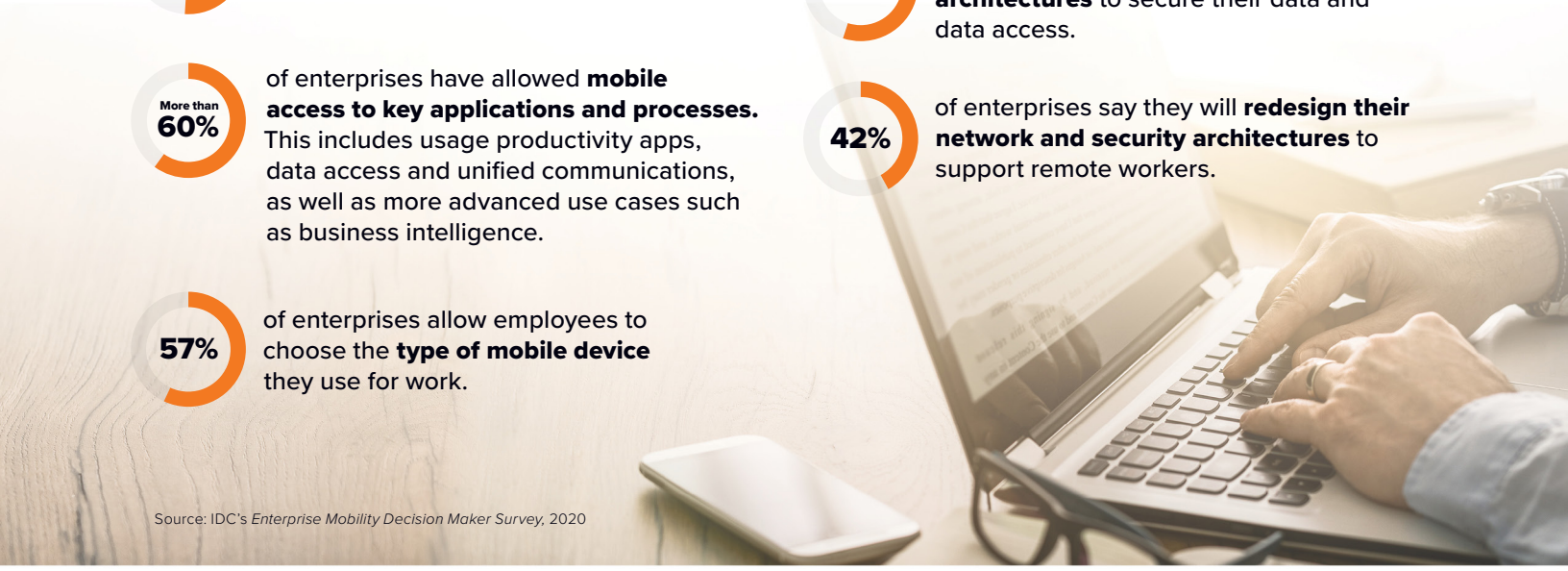
More than 60% of enterprises have allowed **mobile access to key applications and processes.** This includes usage productivity apps, data access and unified communications, as well as more advanced use cases such as business intelligence.

57% of enterprises allow employees to choose the **type of mobile device** they use for work.

52% of enterprises say **usage monitoring and personal data privacy concerns** on mobile devices are the top barriers to enrolling devices in EMM/MDM.

55% of enterprises say they're actively using **modern security principles and architectures** to secure their data and data access.

42% of enterprises say they will **redesign their network and security architectures** to support remote workers.



Source: IDC's *Enterprise Mobility Decision Maker Survey,* 2020

Changes in Mobile and Remote Work Require a New Security Model

More than ever before, enterprise employees are getting work done outside the traditional office perimeter while using mobile devices. A majority of U.S. enterprises say they support partial or full remote work for the foreseeable future.

Organizations now offer workers the choice of either using their own device or choosing the type of device provided to them with a wide range of security and management functions available. Many end users are still wary of traditional heavy-handed device management approaches to both corporate-owned or personal devices. Meanwhile, mobile devices have become a primary attack vector for targeted attempts to compromise data or steal sensitive information.

As a result of these shifts, businesses are rethinking their network access architectures. Doing so will help them support remote and hybrid workers using Android and iOS devices as a primary work device. In addition, the focus of cybercriminals and bad actors has shifted to the mobile vector as businesses see attacks and data theft attempts against workers' mobile devices growing. The new model for securing this kind of environment must separate detection points, policy enforcement, and remediation actions from on-device functions.

They should also distinguish from technologies that rely on perimeter-based security tools. Modern cloud-centric security architectures put security controls, monitoring and remediation closer to the apps that workers use. This enables advanced security functions such as multi-factor authentication and continuous conditional access controls that are based on user and device behavior, health, and context.

In the near future, the "where" (location) and "what" (device type) factors of digital work will matter less. This will accelerate the need for compliance, strong security principles, and cloud-centric data protection strategies. Organizations looking to digitally transform operations and improve employee support in the wake of 2020 and looking beyond, must consider modernizing their mobile security, management, and overall app and data access strategies as an integral part of a broader movement towards organizational resiliency.

In the near future, the "where" (location) and "what" (device type) factors of digital work will matter less.