Who is the Everywhere Enterprise?

Introduction

In March 2020, over a third of the world's population was put into lockdown as the COVID-19 crisis took hold. The pandemic changed the face of society overnight as people stayed at home to deter the spread of the virus.

As a direct consequence of this, the pandemic accelerated an already growing shift towards remote work. Workforces around the world were told they could no longer return to the office and businesses were forced to quickly enable their employees to work remotely. In an instant, the traditional office environment transformed to an 'Everywhere Enterprise,' in which work takes place everywhere and data resides everywhere. In the distributed Everywhere Enterprise, employees work on any device and from any location that maximizes their productivity.

At MobileIron, we wanted to understand the different requirements that each employee has in order to work productively within the Everywhere Enterprise, so we polled 1,200 workers across the U.S., U.K., France, Germany, Netherlands, Australia, and New Zealand in an attempt to find out.

The study's findings revealed that the Everywhere Enterprise is here to stay, with the majority of employees around the world agreeing that they do not wish to return to the office full-time. The study also unveiled a level of disparity when it comes to employees' visions on how they'd like to work in the future, with four distinct personas emerging, each with different productivity requirements.

More than
80%
of employees around the world don't want to return to the office full time.

mobileiron

092920EESR-v1-EN-US

The end of the office?

Just as the advent of mobile and cloud technologies heralded the beginning of the end for the traditional network perimeter, the COVID-19 lockdown may have signaled the end for office working as we know it, as businesses shift towards an "Everywhere Enterprise" model of working. More than 80% of the employees surveyed agree that they don't want to return to the office full-time in the aftermath of COVID-19, having enjoyed the ability to work from anywhere during the lockdown period.

This lack of desire to return to the office could, in part, be put down to the fact that businesses around the world were extremely effective in enabling their employees to work from home at the start of the pandemic. In fact, two-thirds (66%) of survey respondents agree that their employer had the right technologies and solutions in place for them to be able to work from home productively.

72%

of employees agree that their mobile device has been important to ensuring their productivity during lockdown.

The study also emphasized the importance of enterprise mobility in ensuring employee productivity, with almost three-quarters (72%) of employees agreeing that their mobile device has been important to ensuring productivity during lockdown.

However, while employees around the world agree they do not want to return to the office full-time, the study revealed distinctions between how employees would like to work going forward. The research revealed four distinct employee profiles, each presenting their own unique security challenges to IT departments.

The Everywhere Entperise Employee: Emergent Personas

Hybrid Henry:

- Typically works in financial services, professional services, or the public sector.
- Ideally splits time equally between working at home and going into the office for face-to-face meetings; although this employee likes working from home, being isolated from teammates is the biggest hindrance to productivity.
- Depends on a laptop and mobile device along with secure access to email, CRM applications, and video collaboration tools to stay productive.
- Believes that IT security ensures productivity and enhances the usability of devices. At the same time, this employee is only somewhat aware of phishing attacks.

Mobile Molly:

- Works constantly on the go using a range of mobile devices, such as tablets and phones, and often relies on public WiFi networks for work.
- Relies on remote collaboration tools and cloud suites to get work done.
- Views unreliable technology as the biggest hindrance to productivity as this individual is always on-the-go and heavily relies on mobile devices.
- Views IT security as a hindrance to productivity as it slows down the ability to get tasks done; this employee also believes IT security compromises personal privacy.
- This is the most likely persona to click on a malicious link due to a heavy reliance on mobile devices.

Desktop Dora:

- Finds being away from teammates and working from home a hindrance to productivity and can't wait to get back to the office.
- Prefers to work on a desktop computer from a fixed location than on mobile devices.
- Relies heavily on productivity suites to communicate with colleagues in and out of the office.
- Views IT security as a low priority and leaves it to the IT department to deal with. This employee is also only somewhat aware of phishing attacks.

Frontline Fred:

- Works on the frontlines in industries like healthcare, logistics, or retail.
- Works from fixed and specific locations, such as hospitals or retail shops; this employee can't work remotely.
- Relies on purpose-built devices and applications, such as medical or courier devices and applications, to work; this employee is not as dependent on personal mobile devices for productivity as other personas.
- Realizes that IT security is essential to enabling productivity; this employee can't afford to have any device or application down time, given the specialist nature of their work.

mobileiron

Securing the Everywhere Enterprise

The Everywhere Enterprise and its different employee personas pose a significant challenge to IT security teams: how can they secure this new, dispersed workforce? To make matters worse, the study also found that employees within the Everywhere Enterprise are making IT's job harder by not prioritizing, or even circumventing, security protocols. In fact, the study found that one-third of workers (33%) around the world consider IT security to be a low priority.

To add to their woes, it seems that employees within the Everywhere Enterprise are particularly blind to the threats and vulnerabilities that are specifically targeting them. Mobile phishing attacks that target remote and dispersed workers have increased dramatically since workforces were sent home in mid-March. However, nearly half (43%) of the employees said they do not know what a mobile phishing attack is.

So, how do IT departments secure employees in the Everywhere Enterprise? The solution is adopting a mobile-centric zero trust approach to enterprise security. By implementing a zero trust approach – which is more necessary in Covid times than ever before – organizations can ensure that only verified users and trusted applications, devices and networks are being used before granting employees access to the corporate data they need. It is the only way businesses can ensure that their dispersed employees can remain both secure and productive, wherever they choose to work from.

In order to fully ensure that their remote employees are fully protected from the mobile phishing attacks targeting them, organizations should also look to enhance their security infrastructure with mobile threat defense capabilities that detect and remediate against on-device threats, such as phishing attacks. In doing so, IT departments can ensure that their remote employees can access their critical business data wherever and whenever they need to from any device – without putting that data at risk.

For more information about securing the Everywhere Enterprise, visit here: www.mobileiron.com

By combining MobileIron Threat Defense with MobileIron Zero Sign-on, on a secure foundation of MobileIron Unified Endpoint Management (UEM), organizations can detect and remediate mobile threats on device, remove the pain of passwords, and enable secure and seamless access to enterprise data to all who need it, as and when they need it.

mobileiron