Is your organization equipped to manage the new mobile workforce?

Five things every business owner needs to know to manage the new mobile workforce and support their IT department along the way.

2020 was met with uncertainty as many organizations unexpectedly had to pack up their offices and transition to a new work life – at home.

IT staff were strained and struggled to keep workforces up and running, some losing money and time in the process while leaving businesses up to avoidable risks. Businesses small and large made mistakes, learned new ways to operate remotely and embraced industry-wide change for the first time in decades.

As people continue to work from home or adopt a hybrid approach in 2021 and beyond, businesses need to find ways to not just survive but thrive in this new normal. Companies will need to consider how this global shift in mobile workforce management today may affect future plans tomorrow.

In this white paper, we'll take a deeper look at the key trends impacting the future mobile workforce, including:

1. BYOD: Left to Your Own Devices
2. The Value of Virtualization
3. Em'powering' the Next Generation
4. Security Gets Serious
5. The Right Tools Reign Supreme

After reviewing these topics, we'll close it out with a quick predictive look at what's ahead for remote workforce and how you can set yourself up for success now.

1. BYOD: Left to your own devices

Before the pandemic, 17 percent of U.S. employees worked from home 5 days or more per week, a share that increased to 44 percent during the pandemic.

As employees left offices in droves, many organizations were not equipped with the right tools to assist a remote work infrastructure. Thus, many businesses adopted a Bring Your Own Device (BYOD) approach where employees utilized their personal devices—smartphones, tablets, laptops, desktops—to conduct off-site work.

Under the right circumstances, a BYOD program can be quite effective. Did you know employees using their own devices for work actually increase their productivity? It's true. The more they enjoy and understand their device personally and the better they know how to use it, the happier and more productive they will be. Plus, BYOD enables your staff to work more efficiently and with an "always there" aspect—choosing to check email, answer messages, and respond to texts even in their off hours.

But, for a BYOD program to work properly, organizations need to consider establishing a company-wide policy to help them take control and shield them from governance, financial, security and larger device management problems.

The challenge? Doing it yourself can be tricky, often diverting strategic leadership attention to resolving technical issues rather than focusing on big picture, long-term success.

The solution? Utilizing a trusted digital workspace platform, like VMware Workspace ONE, can remove gaps and lags in unmanaged devices, enabling you to securely deliver and manage any app on any device, anywhere—removing big barriers and risks for IT teams. And with more than 43.3% of the global workforce expected to be mobile and relying on digital.

WHY WORKSPACE ONE?

Unified Endpoint Management

Consolidate management silos across mobile devices, desktops, rugged devices and "things." Reduce costs and improve security with real-time, over-the-air modern management across all use cases.

MORE

Intelligence Across Digital Workspace

Aggregate and correlate data across your entire digital workspace to drive insights, analytics and powerful automation of common IT tasks. Improve user experience, strengthen security and reduce costs.

MORE

Virtual Desktops & Applications

Transform traditional VDI and published apps, while providing simplicity, flexibility, speed and scale. Gain a common control plane across the multi-cloud.

MORE

Simplify Zero Trust Security

Combine intrinsic security across devices, users and apps to simplify the enablement of zero trust access control. Industry-leading modern management makes zero trust access models a reality.

MORE

2. The value of virtualization

Whether an organization implements a comprehensive BYOD program or chooses a corporate-owned mobile model, it should consider a solid virtualization platform to manage and support these digital workspaces.

This provides organizations a wealth of benefits, including (but not limited to):

Simplified Management & Scalability: Whether it's 100 or 100,000 devices—phones, tablets, laptops and computers—virtualization enables you to centralize desktop management with quick mobile device deployments and app distribution from a single control plane. VMware Horizon Cloud, for instance, can create a virtual desktop infrastructure (VDI) that supports multitenancy, automated provisioning, and secure data access for your internal workforce, as well as external contractors. Everyone can have all the apps and tools they need to do their job.

Enhanced Security: So how can virtualization ensure corporate data security on personal devices? Instead of data being housed at different endpoints, it's all housed in a central location. This prevents data leaking out at those endpoints since data doesn't exist there. For instance, if a user logs in to their desktop on a random computer, any data is contained inside that virtual desktop can't escape even with admin access. Depending on role configuration of a fully managed device, say for an executive, they could potentially have access to share data with USBs, but for unmanaged and personal devices, that would be blocked. By keeping corporate/sensitive data off endpoints, Horizon Cloud can help you ensure regulatory compliance, while providing secure access to business-critical virtual desktops and apps.

Cost Savings: Horizon Cloud radically transforms traditional desktop and application virtualization with a predictable and flexible cost-model where you're only charged for what you use. This consumption-based model makes it easy for you to plan your monthly budget and benefit from low usage, like when people take off during the holidays. Virtualization also reduces large up-front expenditures for expensive hardware and can streamline management, onboarding and deployment, so your highly paid IT staff isn't responsible for day-to-day tasks.

User Experience: Remote workers expect to be able to work anywhere on any device. Virtualization provides them with the same experience no matter the device. This helps them adapt quicker to the "new normal" without the hiccups of learning something completely new. For the long haul, if there's any issue, like a new hire who hasn't received their computer yet or an existing employee's computer is down, they don't have to wait for new computer or device. They can go to any computer and single sign on to get their work done without waiting.

"With a virtualization platform, like VMware Horizon Cloud, you can deliver, manage, and monitor virtual desktops and applications for users who don't need access to a full desktop."

– Tristan Sitz, Stratix's Technical Presales Engineer

CASE STUDY/SUCCESS STORY:

Utility Company Experiences Real Results with Virtualization

A utilities company had to scramble when state mandates made working from home mandatory last March. Unfortunately, they were nowhere near ready. Instead of using a preinstalled application on their personal PCs, users had to remote into a different PC that's inside the network, which was not only cumbersome, but with multiple users on at the same time creating connectivity issues, it was almost impossible for anyone to work efficiently.

With a cloud-based virtual platform, like VMware Horizon Cloud, the company was able to open access to workers, including making it possible for them to use older applications, using their home devices and without clogging up the network. Virtualizing their systems made a lot more sense than investing in new expensive equipment, building from the ground up, and training their remote workforce to use this new technology.

STRATIX AND HORIZON CLOUD: BETTER TOGETHER

Stratix is here to help carry out the deployment of your virtual environment and provide you with the level of support you need, including fully managed support. Think of our team as your mobile device management assistant, taking on the time-consuming tasks you don't want your higher-level admins doing, including:

> New employee enrollment
>
> Enterprise mobility management support
>
> 24/7 monitoring and management
>
> BYOD policy, patch and advanced configurations support
>
> Telecom expense management
>
> And more

Many organizational leaders are looking to automating mobility management and partnering with managed mobility service providers to handle repetitive and high-volume tasks. However, it's imperative to thoroughly vet providers in their expertise, capabilities and support proficiency.

With Stratix, you can reduce the demand on your IT resources, expand your support capabilities and lower management costs. Find out how we can benefit your business.

3. EmPOWERING the next generation

Something else businesses have to consider as they plan for true mobile transformation is the employees that will make up the new mobile workforce.

Seventy-four percent of the workforce will be comprised of Millennial and Generation Z workers by 2030. As Baby Boomers exit the game and Generation X eyes retirement, employers will need to appeal to this up-and-coming workforce comprised of "digital natives," especially if they want to attract and retain top talent. **Let's take a closer look at what drives these generations' mobile device usage and preferences**:

GENERATION X Born 1965-80	MILLENNIALS Born 1981-96	GEN Z Born 1997-2012
50% agree it's very important for them to have the **latest technological products.**	**74% of the workforce** will be comprised of Millennial and Generation Z workers by 2030.	**One-third** of Gen Z workers who prefer to use a laptop for work want a two-in-one laptop as their next machine.
66% of Gen Xers say that how much an organization embraces technology influences where they decide to work.	Gen X's global mobile internet usage rate is the **second highest**, only behind Millennials' usage rate.	Gen Z workers are **more likely** to work in a variety of locations, such as co-working spaces, while commuting or in multiple locations in the office.
Today, **55% of Gen Xers** say they own tablets	**1 of 2 millennials** purchase their device for the camera quality.	Younger workers are more likely to **dodge security policies** in the name of productivity.
More than other generations, Gen Zers and Millennials choose smartphones for the design/color and multimedia capabilities.	**58% are working from home** full or part-time	**23% of Gen Zers** are concerned about their company accessing personal data on personal devices they use for work, compared with just 14% for Gen Xers and 9% for baby boomers.
	68% of Millennials are happier working remotely, while Baby Boomers are the least happy with remote work (37%).	

4. Security gets serious

As these "digital natives" and younger generations opt to utilize personal devices for work, especially in a BYOD working environment, employers will need to consider investing in safer, more secure mobile device management solutions—sooner rather than later.

Without proper planning and policies in place, businesses can be at risk for things like data breaches. Something as simple as transferring company files onto a public cloud storage service, pasting confidential info in the wrong place, or forwarding an email to an unintended recipient are more likely to happen using a personal device. To add to that, let's not forget, insufficiently secured personal devices and home routers and unsanctioned channels (such as apps, personal email and cloud-based document processors), also play a key role in falling victim to these data breaches.

If you're wondering what devices are most at risk, users are most likely to first encounter messages on their smartphone versus their PC. The limited display area, with smaller wording and larger buttons, makes users three-times more likely to respond to phishing attacks on smartphones versus PCs. What makes this even worse is the way people often multi-task while using their devices which amplifies the effectiveness of the attack.

Another inroad to your data is through rogue apps. Whether looking for an app to increase device functionality or an app to improve work-from-home productivity, users open the door to cybercriminals through side-loaded apps, which can secretly upload data for hackers to exploit. Only 3% of businesses totally block users from installing any apps and less than half of companies limit their users' ability to install apps from recognized stores, such as Apple App Store and Google Play Store.

Situations like this make mobile device security 2021's fastest growing cybersecurity category. It's no surprise that there is a greater demand for mobile computing security solutions and services.

"Mobile devices are just the entry points for most attacks. Hackers are targeting your servers and databases since that's where your data lays. If you've built an intelligent, secure infrastructure with properly managed systems, you most likely are in a good place. But don't forget, attacks are getting smarter, turning your employees' smartphones into tools they can use to wreak havoc."

– Tristan Sitz, Stratix's Technical Presales Engineer

5. The right tools reign supreme

The tools in your pack are only as good as the abilities they give you to reach your goals.

The tools in your pack are only as good as the abilities they give you to reach your goals. For example, in a recent survey, 49% of respondents from North America expect spending on information technology to increase in 2021. It makes sense considering this investment on information technologies will accelerate organizations' digital transformation. Specifically, businesses are going to invest in enterprise software, devices, IT services, and also communication and collaboration platforms and services.

On the employee side, 44 percent of respondents in a recent survey state that their organizations' employees demand a greater surplus of digital alternatives. This highlights the importance of ensuring that employees have a range of applications and technologies to choose from when working remotely.

Considering all this, you may be asking yourself what your company really needs to satisfy everyone in the mobile workforce equation.

The short answer? A scalable, secure Mobile Device Management (MDM) solution with a solid digital workspace that brings flexibility (and peace of mind) to the IT department and end users.

U.S. EXECUTIVES ARE PLANNING TO MAKE NEW INVESTMENTS TO SUPPORT HYBRID WORKING

74% plan to increase investment in tools for virtual collaboration

70% in IT infrastructure to secure virtual connectivity

64% in training to manage a more virtual workforce

57% in conference rooms with enhanced virtual connectivity

50% in hoteling applications

Source: Society for Human Resources Management (SHRM)

What's on the horizon for remote work?

We may have all finally hit our stride, but if we've learned anything from the past year, it's to not get too comfortable. To maintain (and inevitably outgrow your organization's moble IT infrastructure, enlist a trusted advisor and partner like Stratix to help manage the process.

Stratix has the expertise to help your business achieve your mobility goals. As a leading managed mobility service provider, Stratix's certified experts have seen and solved every mobile device management challenge.

Considering an Mobile Device Management upgrade, implementing a BYOD policy or looking for a Virtual Desktop Infrastructure (VDI) solution? Stratix experts, along with key partners like VMware, can help roadmap your mobility transformation journey, so you're not making a decision now that will leave you stuck later. Stratix is enterprise-ready and scalable to fit your needs.

Together, we can:

> **Build and effectively manage mobile** processes, including security protocols, application deployment, update management, training and documentation and user support
>
> **Keep corporate content secure** while also providing employees with the access they need to do their jobs
>
> **Create and enforce mobile policies** to mitigate the risks involved with BYOD connecting to your enterprise networks
>
> **Capitalize on your evolving mobility business,** accelerate corporate growth and achieve long-term success

About Stratix

As the most experienced pure-play enterprise mobility specialist in the U.S., Stratix is dedicated to guaranteeing nonstop mobility. The company leverages four decades of expertise to accelerate and inspire mobility transformation for some of the world's largest organizations. Stratix's SmartMobile programs ensure each client has the right technology, tools, and support programs in place to stay ahead. For additional information, visit **www.stratixcorp.com**

Contact Us: 800-883-8300

Connect with us: