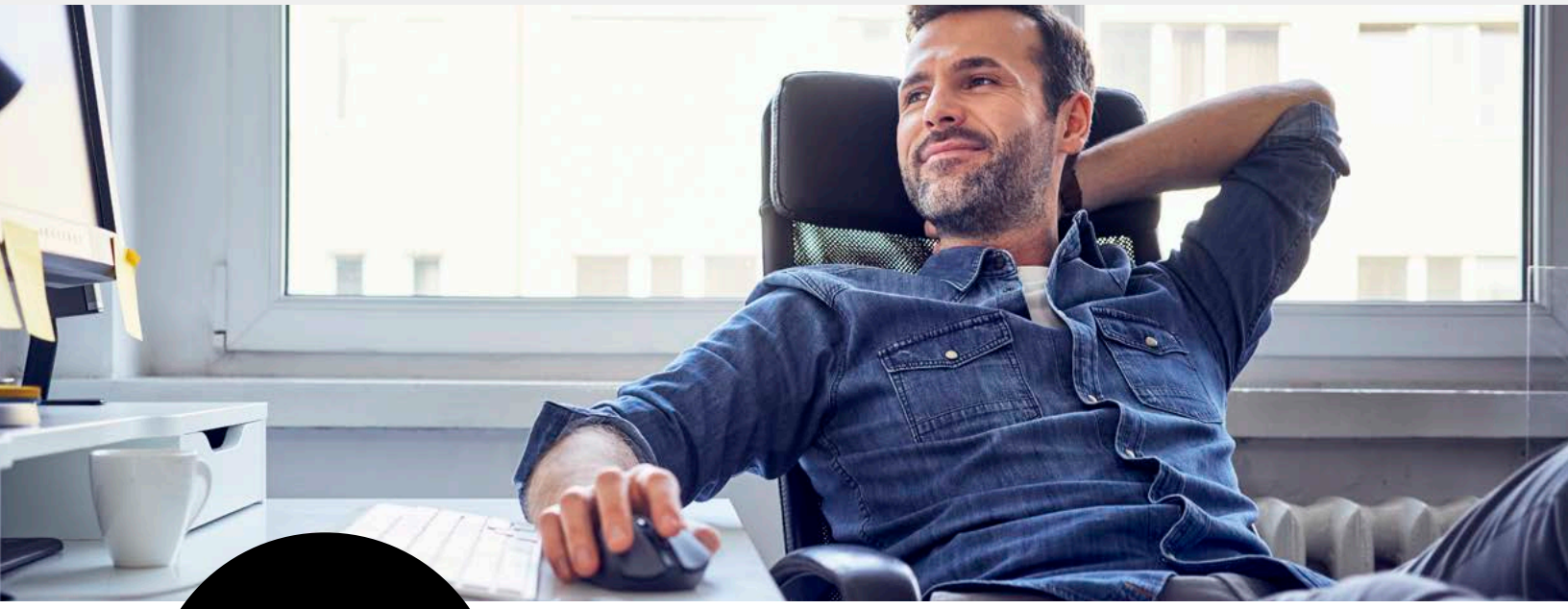
Empowering today's anytime-anywhere workforce

Tasked with supporting at-home workers on an unprecedented scale during the coronavirus shutdown and anticipating future remote strategies, 56% of IT leaders report that they plan to outsource more.[1]



51%

of office workers are now doing their jobs entirely from home[1]

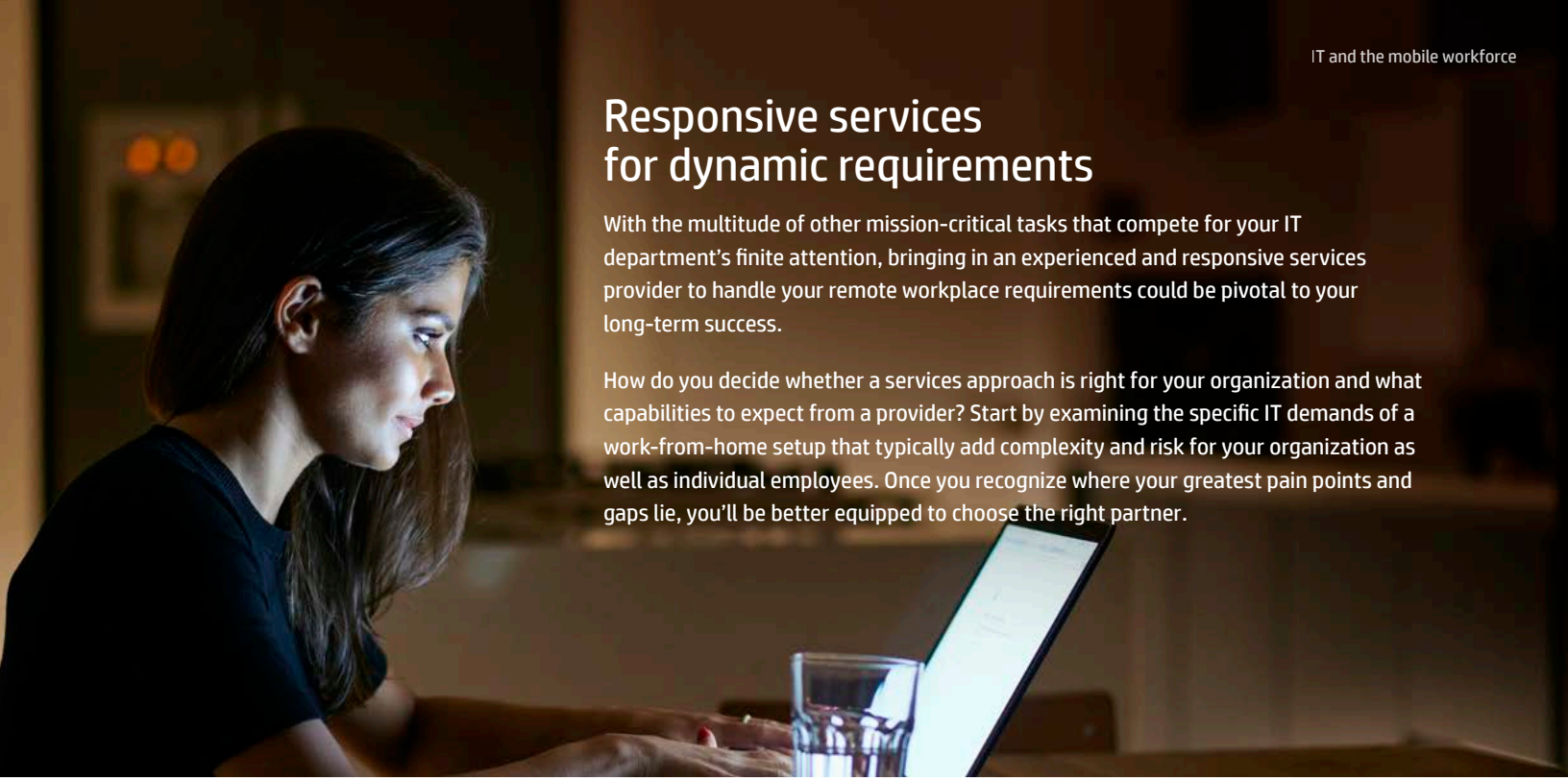
98%

of remote workers around the world would like to continue doing so, at least part-time, for the rest of their careers[4]

Almost literally overnight in spring 2020, working from home morphed from an option to an outright necessity as organizations around the world closed their offices amid the COVID-19 health crisis. An estimated 62% of employed Americans were doing their jobs remotely as of April 2, 2020—up from about 31% just two weeks earlier.[2] Globally, 88% of organizations had encouraged or required their employees to work from home.[3]

Although this event intensified the pressure on IT teams and executives to ramp up new or expanded support for remote workers, the work-from-home movement had already been accelerating steadily since the start of the new millennium. Many organizations are now using the experience gained from COVID-19 to shape their plans for addressing longer-term remote workforce needs and opportunities.

Organizations that invested in cloud-based workplace and remote access capabilities prior to the COVID-19 crisis are adapting more readily than those with systems that were designed mainly for corporate network usage. Both now and in the long term, the advantages of enabling employees to work productively, securely, and happily—from anywhere and at any time they choose—have never been clearer.



Responsive services for dynamic requirements

With the multitude of other mission-critical tasks that compete for your IT department's finite attention, bringing in an experienced and responsive services provider to handle your remote workplace requirements could be pivotal to your long-term success.

How do you decide whether a services approach is right for your organization and what capabilities to expect from a provider? Start by examining the specific IT demands of a work-from-home setup that typically add complexity and risk for your organization as well as individual employees. Once you recognize where your greatest pain points and gaps lie, you'll be better equipped to choose the right partner.

Devices that fit—and improve—how employees work

As more employees access corporate networks, applications, data, and support from remote locations—often on personal devices such as smartphones and notebooks—the IT team can easily get immersed in competing challenges. You may need to configure new devices for at-home use, field more IT helpdesk requests, and roll out additional remote collaboration tools so employees stay productive. On top of these and other demands, your IT department is still tasked with actively managing costs.

85%

of business leaders say employee productivity has increased in their business as a result of providing greater flexibility to work outside the office[5]

When evaluating service providers to help keep your devices functioning optimally and your employees working happily, look at the types of support you'll receive at every stage of the device lifecycle. Not all vendors deliver a complete portfolio of services that can effectively free your in-house IT team to focus on core business tasks.

Ask the provider:

- Can you help assess my current IT environment and advise on whether to migrate existing devices or purchase new hardware?
- Do you provide pricing models to purchase as-a-Service with flexible scalability?
- Are you able to configure devices and applications at the factory prior to shipment?
- How will you deploy new devices and services quickly, with minimal disruption to employee productivity?
- Can you support different needs across multiple regions and tailor services to local requirements?
- What tools do you provide for optimizing system performance and maintaining our device infrastructure?
- How will you manage end-of-life needs such as device recovery, deinstallation, secure data erasure, and equipment recycling?

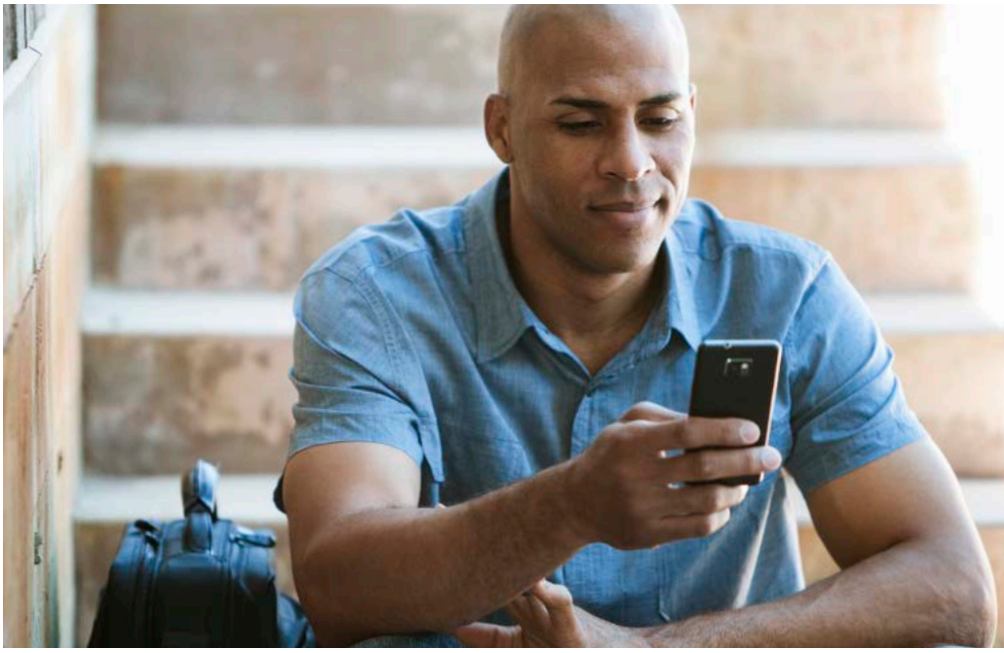
Manageability that stays a step ahead of user needs

Moving your organization's IT environment to the cloud not only opens greater opportunities for employees to work remotely but also gives them access to a broader array of technologies and more satisfying ways to collaborate. However, the related demands of managing additional end-user devices with multiple operating systems (OSs) could overwhelm an already time- and budget-strapped IT team.

Many organizations are bringing in a service provider to help automate device management tasks and use analytics platforms to resolve issues before they affect employees. This type of arrangement really starts to make business sense when a provider can demonstrate that its services will reduce overall costs, complexity, and in-house support across a cloud-based environment.

48%

of Americans spend an hour or more per day checking their cell phones for work-related reasons[6]



Some important considerations include:

- How extensively will this service provider monitor my device health and security?
- Will I receive actionable insights into the performance of users' notebooks, workstations, and mobile devices across my multi-OS environment?
- Can the provider analyze and report on which devices are connected to my network and what apps are installed on them?
- Will I receive fast and complete details on the causes of system errors or crashes?
- How does the provider stay on top of whether connected devices comply with my organization's security policies?

Security that goes where data, devices, and employees do

Safeguarding devices and data against increasingly sophisticated cyberattacks as well as accidental breaches is a perennial focus for IT professionals. The security challenges multiply as employees spend more time working remotely. Potential risks emerge whenever someone logs into the corporate network using a personal device, accesses sensitive information on home or public Wi-Fi connection, or travels with a company-issued device.

To be effective, you need a security approach that protects your organization without adding complexity to employees' roles or impeding their productivity. You also have to balance your IT team's security work alongside myriad other priorities.

Here are some key areas to explore:

- Can this security services provider help add defenses around my remote work environment quickly—without increasing the in-house IT workload?
- Does the provider offer integrated protection across endpoint devices, cloud-based applications, network hardware, and web touchpoints?
- Does the provider have a deep bench of security experts, and how much ongoing support will my IT department consistently receive from them?
- Can I count on these services to proactively identify and resolve potential security risks before they cause actual damage?
- What's the provider's approach to keeping security unobtrusive for employees so they can stay focused on their day-to-day work?

When IT does more, so can your employees

Organizations of all sizes are discovering the benefits of adopting managed services to support an increasingly mobile and remote workforce. When you're ready to expand the possibilities for device deployment, management, and security across your organization, HP Services can help assess your specific requirements and line up potential solutions.

We have decades of experience meeting the needs of customers in all industries through:

- **HP Lifecycle Services** that help keep employees happy, productive, and more engaged—by improving how they work
- **HP Manageability Services** that reduce the cost and complexity of managing end-user devices and simplify IT workloads—enabling a better employee experience
- **HP Security Services** that comprehensively protect devices and data against threats—allowing employees to work when and where they want, without putting the organization at risk

HP Services helps businesses adapt and compete as circumstances change – which is even more important in uncertain times. With HP, IT can focus people and resources on the things that drive business forward.

Sources:

1. *HP Proprietary Research, 2020.*
2. *Gallup Panel, conducted March 30-April 2, 2020.*
3. *Facility Executive, "Most Employees Are Working From Home Due To COVID-19," March 19, 2020.*
4. *Buffer, State of Remote Work Report 2020, May, 2020.*
5. *IWG, Global Workspace Survey, March 2019.*
6. *Wilson Electronics, The Cell Phone Habits of the Typical American at the Workplace, September 17, 2019.*
7. *Wandera, Understanding the key rends in mobile enterprise security in 2020, accessed April 20, 2020.*

To learn more about HP Services, visit www.hp.com/hp-services

4AA7-7551ENW, Rev 2, January 2021