

# Meeting the same IT goals in a whole new work world

How can the new tech help you keep employees  
happy and productive in the hybrid work age?



# A new phase is washing over the workplace: hybrid



By July 2021, 92% of IT leaders reported that they were planning to move to a hybrid model or had already done so.<sup>1</sup> That means more employees began mixing their time between the office, home office, and co-working locations. And although 57% of IT leaders said they were excited about the prospects,<sup>1</sup> and 44% felt that it was a move in the right direction,<sup>1</sup> 78% also predicted this shift would become a burden for IT.<sup>2</sup>

Many organizations are now using the experience gained from two years of global business disruption to shape their plans for longer-term hybrid workforce needs and opportunities. And they've come to realize something: Their IT teams simply can't do it all on their own. Sometimes they need supplemental services to cover all the bases they just don't have the bandwidth for.

Companies are learning that outsourcing to a cloud-based platform supported by expert IT services creates a digital ecosystem where workers can move seamlessly among environments.

**68%** of American workers say the ability to work remotely and on-site is the perfect work model<sup>3</sup>

**70%** of companies expect a blend of in-person and remote working going forward<sup>4</sup>

**63%** of high-growth companies embrace hybrid work models<sup>3</sup>

Organizations are realizing the freedom that forms from a technology biome where IT can manage devices with the power, efficiency, and visibility of tools including global telemetry, machine learning, and predictive analytics. By automating and offloading the tedious, time-draining tasks, they're increasing employee productivity and preventing IT staff burnout.



# Services that fill specific needs



A multitude of mission-critical tasks compete for your IT department's finite attention. Bringing in an experienced and responsive services provider to give them some relief in handling your hybrid workplace requirements could be pivotal to your organization's long-term success.

But how do you decide whether a services approach is right for your organization, and what capabilities should you expect from a provider? Start by examining the specific IT elements of a work-and-collaborate-from-anywhere setup. Whatever their benefits, these flexible arrangements add complexity and risk for both the organization and individual employees.

After you recognize where your greatest pain points and gaps lie, you'll be better equipped to choose the right partner to enable your business growth.

**3.5%** of service providers polled by Forrester expect an uptick in client agreements emphasizing outcome-based delivery<sup>5</sup>

**85%** of businesses have somewhat or greatly accelerated the implementation of technologies that digitally enable employee interaction and collaboration<sup>6</sup>

**Only 38%** of employers have upgraded their video technology to allow for more hybrid collaboration<sup>7</sup>



# Devices that fit how employees work



As more employees access corporate networks, applications, data, and support from remote locations—often on personal devices such as smartphones, laptops, tablets, and printers—your IT teams can easily get immersed in competing challenges.

They may need to configure new devices for at-home use, field more IT help-desk requests, and roll out additional remote collaboration tools so employees stay productive. On top of these and other demands, your IT managers are still tasked with actively managing costs.

Adding supplemental support services can help you preserve the well-being and satisfaction of your existing IT team at a lower cost than adding more full-time staff, especially in a time when the hiring market is so challenging.

When evaluating managed service providers to help keep your devices functioning optimally and your employees working happily, look at the types of support you 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.

Here are some important questions to help select a potential services partner.

---

Can you help assess my current IT environment and advise me on moving to a modern endpoint management approach?

---

Do you provide pricing models to purchase as-a-Service with flexible scalability? Do you configure devices and applications at the factory prior to shipment?

---

How do you deploy devices and services quickly, with minimal disruption to employee productivity, wherever they work?

---

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?

---

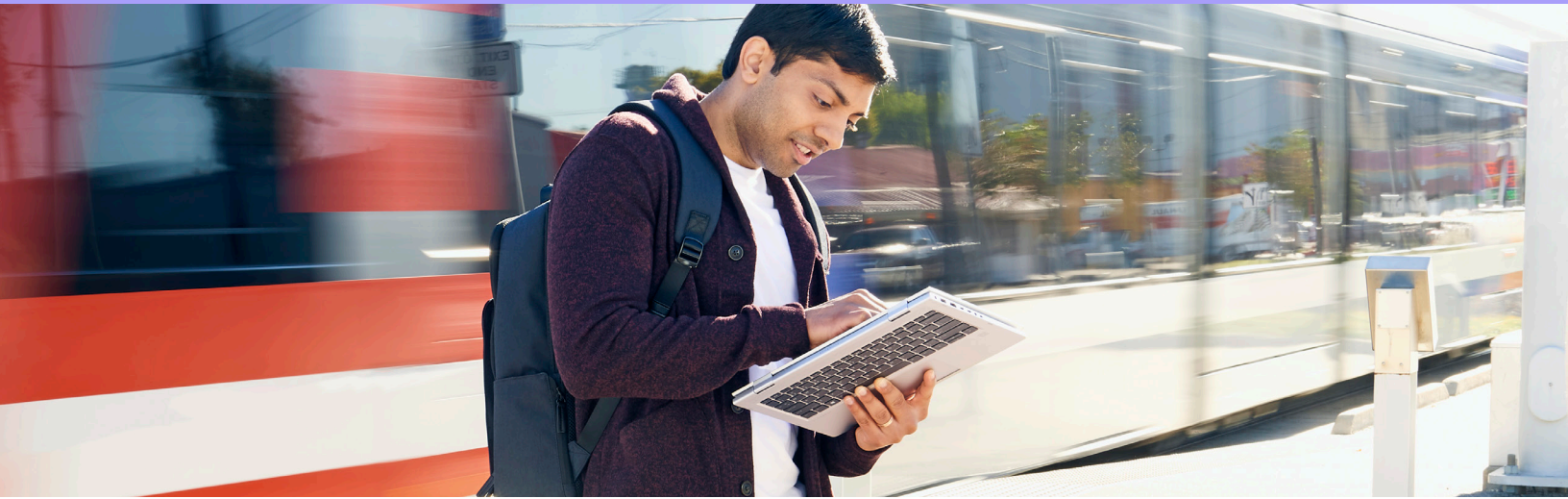
How do you manage end-of-life needs such as device recovery, deinstallation, secure data erasure, and equipment recycling?

---

**85%** of CIOs say employees are just as productive working remotely as in the office<sup>2</sup>



# Device management that stays a step ahead of user needs



Moving your organization's IT environment to the cloud gives IT more effective ways to support employees who are working remotely or moving between remote and on-site work environments.

This model also gives workers access to a broader array of technologies and more satisfying ways to collaborate. However, the related demands of managing additional end-user devices can overwhelm an already time- and budget-strapped IT team.

Bringing in a service provider can help your IT team keep up by automating device management tasks and using analytics platforms to resolve issues before they affect employees.

This type of cloud-based arrangement truly starts to make business sense when a provider can demonstrate that its services reduce overall costs and complexity, as well as ease the staffing challenges involved in conducting in-house support.

**88%** of IT leaders believe that it's essential for employees to effectively and efficiently work remotely<sup>2</sup>

Here are some important considerations.

---

How extensively will this service provider monitor my device health and security?

---

Will I receive actionable insights into the performance of users' notebooks, workstations, printers, mobile devices, and even conferencing solutions across my multi-OS environment?

---

Will I be able to monitor and manage which devices are connected to my network and what applications are installed?

---

Can the provider help me set up paper-based, cloud-integrated workflows for the digital world?

---

How quickly will I receive complete details on the causes of system errors or crashes?

---

Do you have predictive analytics capabilities to identify issues before they become problems?

---

How does the provider stay apprised of whether connected devices comply with my organization's security policies?



# Security that goes where your people and devices go



62% increase in ransomware attacks in 2021<sup>8</sup>

54% of IT professionals consider remote workers to pose a greater security risk than traditional workers<sup>9</sup>

75% of IT leaders say their organizations have increased spending on security tools in the last 12 months<sup>2</sup>

Safeguarding devices and data against increasingly sophisticated cyberattacks as well as accidental breaches is a perennial focus for IT professionals, but that focus has magnified with the move to hybrid work. Security challenges multiply as employees spend more time working remotely or moving between locations. In the last month of 2021, organizations worldwide experienced more than 722 million attacks in 30 days.<sup>10</sup>

Potential risks emerge whenever someone logs in to the corporate network using a personal device, accesses sensitive information on home or public Wi-Fi connections, installs unauthorized applications, or travels with a company-issued device.

Going with a BYOP (bring-your-own-printer) approach serves up additional risks, falling under the dreaded umbrella of shadow IT. Though it keeps printer management out of IT's work queue, employees' personal printers won't have the proper security configurations and business policies applied for information to be shared safely.

Security Magazine notes, "The use of unauthorized software and shadow IT can also jeopardize a business's entire cybersecurity posture."<sup>11</sup>

It's inevitable that something will slip through—unless you deploy an always-on, always-watching sentinel of tools and services that has IT's back, reducing risk and stress.

To be effective, you need a security approach that protects your organization without adding productivity-impeding complexity to the workday for employees or IT. 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 add a multilayered defense to 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 is the provider's approach to keeping security unobtrusive so employees can stay focused on their day-to-day work?



# Give employees and I.T. the right tools and help keep employees feeling and working their best—wherever they are.

IT's work is business-critical. That's why organizations of all sizes are discovering the benefits of adopting managed services to support the PCs, printers, smartphones, conferencing solutions, and other endpoints that are relied on so heavily by an increasingly hybrid workforce. Augmenting your IT department with HP Services can help you reinvent how you work—freeing both workers and IT to get the job done comfortably, anywhere, anytime.

**FREEDOM FOR WORKERS** with **PERSONALIZED** solutions that accommodate diverse needs, locations, and work styles: versatile devices, immersive experiences, ergonomic support, and cloud-enabled tools.

**FREEDOM FROM GROWING THREATS** with solutions that leave you **PROTECTED** against security risks aimed at your people and your data: zero trust, isolation and containment, automatic updates, and managed services.

**FREEDOM FROM IT OVERLOAD AND BURNOUT** with solutions that make your IT teams more **PRODUCTIVE** amid growing demands and responsibilities: IT automation, digitized workflows, modern management, and remote configuration and deployment.

**FREEDOM TO MEET CHANGING BUSINESS DEMANDS** with solutions that get you **PREPARED** to address the specific goals of your IT teams and your business: real-time insights, configurable solutions, and endpoint and lifecycle management.

Give IT the extra support they need to make hybrid work less of a burden on their day.

Learn more at [hp.com/hp-services](https://hp.com/hp-services) —>

<sup>1</sup> Snow Software, "Study: Hybrid Work Is Here to Stay, Bringing Its Own Mix of Complexities," July 29, 2021, <https://www.snowsoftware.com/blog/study-hybrid-work-here-stay-bringing-its-own-mix-complexities>

<sup>2</sup> Snow Software, "2022 IT Priorities Report," December 2021, [https://go.snowsoftware.com/rs/377-PWR-208/images/2022\\_Snow\\_IT\\_Priorities\\_Report\\_12.6.21\\_FINAL.pdf](https://go.snowsoftware.com/rs/377-PWR-208/images/2022_Snow_IT_Priorities_Report_12.6.21_FINAL.pdf)

<sup>3</sup> Apollo Technical, "19 Important Hybrid Working Statistics to Know Now and for the Future (2021)," January 6, 2022, <https://www.apollotechnical.com/hybrid-working-statistics>

<sup>4</sup> CNBC, "The latest numbers on how many workers will be returning to offices, and how often," July 8, 2021, <https://www.cnbc.com/2021/07/08/how-many-workers-will-be-returning-to-offices-and-how-often.html>

<sup>5</sup> Forbes, "5 Ways To Support Hybrid Working In The Future Workplace," March 15, 2021, <https://www.forbes.com/sites/nigeldavies/2021/03/15/5-ways-to-support-hybrid-working-in-the-future-workplace/?sh=4cefa823373d>

<sup>6</sup> The Enterprisers Project, "Hybrid work's next phase: 3 lessons for CIOs," October 29, 2021, <https://enterpriseproject.com/article/2021/10/hybrid-work-next-phase-3-lessons>

<sup>7</sup> Owl Labs, "New Hybrid Work Statistics: The 5th Annual State of Remote Work Report," November 11, 2021, <https://resources.owlabs.com/blog/state-of-remote-work-report-2021>

<sup>8</sup> Intras Cloud Services, "5 Ways to Protect Yourself from Cyber Security Threats in 2022," January 2, 2022, <https://www.intrasclooudservices.com/blog/5-ways-to-protect-yourself-from-cyber-security-threats-in-2022/>

<sup>9</sup> Findstack, "The Ultimate List of Remote Work Statistics for 2022," December 6, 2021, <https://findstack.com/remote-work-statistics>

<sup>10</sup> Cybercrime Magazine, "Organizations Worldwide Experience Over 722 Million Attacks In The Last 30 Days!" December 29, 2021, <https://blog.knowbe4.com/organizations-worldwide-experience-over-722-million-attacks-in-the-last-30-days>

<sup>11</sup> Security Magazine, "Top 5 cybersecurity challenges in the hybrid office," June 16, 2021, <https://www.securitymagazine.com/articles/95434-top-5-cybersecurity-challenges-in-the-hybrid-office>

HP Services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

© Copyright 2022 HP Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

