EBOOK

MANAGING IT FOR A HYBRID WORKFORCE

Introduction

As we slowly and hesitantly venture out of our homes into public spaces and offices, the buzzwords on everyone's lips seems to be "hybrid work." A hybrid work arrangement is one in which employees work from the office on some days and from home on other days. A recent Accenture survey revealed that 83% of respondents preferred a hybrid work model while about 63% of high-growth companies have already adopted a "productivity anywhere" workforce model.

According to numerous management consultants, hybrid work was on track to become the next big workplace trend, and while they expected it to take hold in five to ten years, the Covid-19-pandemic-induced lockdowns got us there sooner.

While companies are encouraging their staff to return to work due to the slowing down of the pandemic, employees are opposing the demand since they want to continue enjoying the work-life balance and safety afforded by remote work. Moreover, businesses have also observed that their employees were more productive and happy working remotely during the pandemic.

According to an academic survey, six out of ten workers said they were more productive working from home. The study found that respondents' productivity at home was, on average, 7% higher than they expected. About 40% of workers reported being more productive at home than in the office during the pandemic, with just 15% stating the opposite.

While remote work has many benefits, many jobs call for employees, such as cashiers at retail outlets, receptionists, IT technicians, to work on-site full-time or most of the time. Thus, to better meet the demands of employees, many companies are adopting a hybrid work model to give employees the option of working in an office as well as from home, as needed.

In this eBook, we'll examine the nature and requirements of hybrid work models from an IT perspective. The IT infrastructure used for a full on-site office environment will not be ideal for running a hybrid environment safely and efficiently. This eBook will answer questions around what changes IT teams should implement to unlock the true potential of a hybrid environment.

What is a hybrid work model?

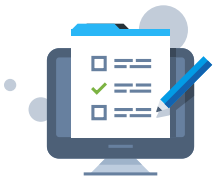
To put it simply, a hybrid work model means having the flexibility to work from anywhere at any time. However, the hybrid structure of each company differs depending on its unique requirements, processes and goals.

For example, some companies may allow employees to work remotely and from the office as per their choice, while others may set limits about the number of days an employee may work remotely. The Microsoft survey found that over 70% of workers want flexible remote work options to continue while more than 65% want more face-to-face time with their team.

A hybrid work model offers flexibility in terms of working hours as well. In addition to allowing employees to work from multiple locations, some companies even allow employees to choose their own working hours. More than 52% of respondents to a McKinsey survey want a hybrid work environment post-pandemic as opposed to 30% in pre-pandemic times.

The policy of worktime flexibility allows employees to complete their work over the day instead of putting in eight or nine hours at a stretch. This is called time slicing. Time slicing helps ensure better work-life balance, especially for employees who are the primary caregivers in their families.

In the wake of the pandemic, many employees have categorically refused to return to work if a hybrid work model is not provided. With over 40% of the global workforce considering leaving their employers in 2021, a thoughtful approach to hybrid work will be critical for attracting and retaining diverse talent. While remote work has proven to be beneficial for companies in the past two years, their next step should be to improve the security and robustness of their IT infrastructure by making it hybrid friendly.



More than **52% of respondents** to a McKinsey survey want a hybrid work environment post-pandemic as **opposed to 30% in pre-pandemic times.**

Over **70% OF WORKERS** want flexible remote work options to continue while **more than 65%** want more face-to-face time with their team.

The challenges of a hybrid work environment

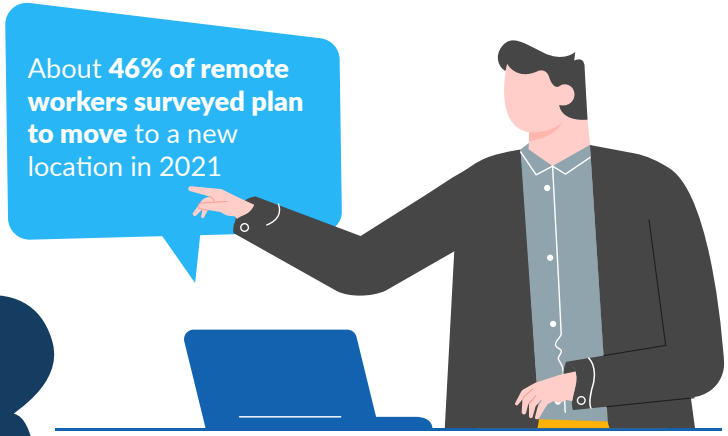
With workforces returning to offices and companies looking to adopt a hybrid work model, businesses need to help their employees and clients deal with a new set of IT challenges. This section discusses some of them.

1. Managing a dispersed workforce

Although companies are willing to adapt their IT environments according to a hybrid setup, bringing a distributed workforce together isn't easy. Managers and CIOs face the challenge of creating an inclusive and collaborative workplace that offers equal opportunities to both in-office and remote workers. This shift to remote work broadens the talent market. About 46% of remote workers surveyed plan to move to a new location in 2021 since they can now work remotely.

Technology will play a key role in creating a work culture where remote employees can interact with their co-workers in the same way as those present in the office. In recent years, most companies have invested in team collaboration tools, video conferencing solutions, interactive digital whiteboards, and other such tools to drive employee engagement and participation even in a remote setup. The video conferencing market size exceeded $15 billion in 2020 and is projected to expand at around 23% CAGR from 2021 to 2027. In addition to ensuring seamless collaboration and communication, the right technology tools can also enhance productivity. The U.S. video conferencing market is forecast to register a growth rate of above 19% through 2027, led by the growing adoption of cloud-based solutions.

Communication is especially crucial in the initial stages of hybrid adoption when processes are likely to be confusing and chaotic. In a hybrid work environment, employees must know how to use devices and software properly to ensure smooth operation. Additionally, they must be taught best practices for protecting their work ecosystems against cyberattacks.



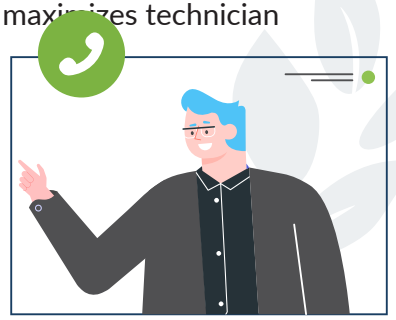
2. Managing remote endpoints

Remote work brought to focus the importance of remote endpoint management, making it a priority for IT departments. The global market for unified endpoint management is forecast to reach $18.9 billion by 2026, growing at a CAGR of 13.2%, helped by cloud-based applications and an increase in cybercrime.A remote endpoint management device is essential to managing a hybrid environment where employees connect to the company's network from various locations, using different networks and devices.

Any device that is connected to a network and that shares and communicates over the network is an endpoint. Workstations, laptops, smartphones, tablets, and even servers, POS systems and internet of things (IoT) devices can be considered endpoints.

Using a unified remote monitoring and management (uRMM) solution, IT teams can view and manage all the devices connected to the company's network from one interface. In addition to adding, removing and configuring devices remotely, IT technicians can use a uRMM tool to patch applications and operating systems, enforce security policies and manage networks. It undertakes all activities and tasks necessary for ensuring the health, safety and functionality of endpoint devices.

Using a uRMM tool, such as Kaseya VSA, you can provide your organization with a complete solution stack that maximizes technician efficiency and enables your business to be successful and more productive.



3. Securing remote endpoints

Since the start of the COVID-19 pandemic, the number of cyberattacks has increased exponentially. During the pandemic, the average cost of a data breach soared to $21,659 per incident according to a new Verizon report. However, about 5% of successful attacks cost businesses over $1 million.

The move to a remote work environment created many vulnerabilities in the IT systems of companies, opening the way for cybercriminals to exploit them. With cybersecurity as the top agenda for companies in this year and the next, the need for endpoint management tools has grown even stronger.

5% of successful attacks cost businesses **over $1 million.**

In addition to managing endpoints, a top-of-the-line uRMM solution will ensure the safety of those devices against cyberattacks. Technicians can use the tool to deploy and update antivirus and antimalware solutions that serve as the first line of defense against cyberattacks. Additionally, uRMM tools ensure timely patch management for Windows and macOS platforms as well as applications used in the workplace.

When left unpatched, vulnerabilities can become doorways to a zero-day attack. Cybercriminals can use zero-day attacks to spy on a company's activities, steal information or compromise the integrity of its IT infrastructure for long periods of time without being detected. Financial losses from cyberattacks are crippling but the loss of trust among employees and clients is harder to restore.

It's impossible for IT technicians to manage each remote endpoint individually or to see which devices are being used at what times, so an endpoint management tool does the work for them. The software detects suspicious behavior, identifies viruses, malware and other risks, and even mitigates them. With applications, tools and work moving to the cloud, and the adoption of digital technologies picking up, endpoints have become a necessity for all organizations.

4. Supporting mobility

Employees are increasingly using mobile devices to perform their work. Because employees will be working remotely, at least some of the time, in a hybrid work setting, it is imperative for companies to make sure all the devices their employees use for work are configured according to IT and security policies.

Cybercriminals can use **zero-day attacks**to spy on a company's activities.

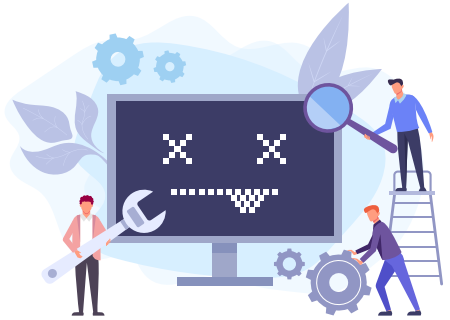
Additionally, due to the rapid technological advancements in mobile devices, it is not uncommon for employees to use more than one device for work or upgrade their systems frequently to increase productivity. The ability to support and service employee devices from anywhere is essential to maintain a healthy hybrid work environment. According to Mordor Intelligence, the enterprise mobility management market was valued at $5.79 billion in 2020 and is projected to reach $11.96 billion by 2026.

In fact, several companies are now considering implementing a BYOD policy, which allows employees to bring their own devices to work. After familiarizing themselves with their personal devices, employees want to continue using them at work. They can then do their jobs more effectively and efficiently. Therefore, organizations benefit from employees producing better quality output in addition to working faster with top-tier devices and tools. Also, this helps with smooth remote onboarding and offboarding practices where employees want to use a device of their choosing.

5. Providing support for broken devices

Devices breaking down, wearing out or becoming obsolete are all part of work life. When all employees were on-site, it was easier and faster to repair malfunctioning devices. Also, this ensured that any sensitive company information did not fall into the hands of a third party during the repair process.

When companies use a hybrid work model, they need to establish policies for supporting and repairing damaged devices. Do employees have to bring their devices to the office IT team for repairs or can they use a private vendor? If employees use their personal devices instead of company-supplied ones, what will the rules be?



In addition, there are repair costs to consider. In the case of personal devices, who pays for repairs? Employees working in a hybrid environment may also have relocated far away from the office. This introduces additional costs and complexities. How are repairs handled in this instance?

Before implementing a hybrid work environment, companies should consider these questions and put down clear guidelines.

6. Managing work-time flexibility

A major reason why employees are pushing their companies to adopt a hybrid work environment is to enjoy and take advantage of work-time flexibility. U.S. workers now prioritize work-life balance and flexibility as the most important factors when evaluating job offers. According to an EY survey, approximately half (54%) of employees surveyed around the world would consider leaving their job if they are not given some flexibility in where and when they work. A hybrid work model enables employees to work when they are most productive rather than being expected to work between 9 am and 5 pm each day. On average, employees want to work between two and three days remotely after the pandemic.

Flexible working arrangements have shown to enhance employee retention, productivity and attendance, while also contributing to a more positive and collaborative work environment. Approximately 67% of survey respondents believed that productivity could be accurately measured regardless of location. While some employees prefer flexible work hours, others prefer to be at work and meet people, seeking out the personal touch and sense of community that happens when we're in the office.

Consequently, companies interested in embracing hybrid work models should approach work-time flexibility in a way that meets their business needs while keeping employees happy.

The planning stage is the best time to address all the above topics to ensure a smooth and straightforward hybrid rollout.

How you can leverage IT to manage a hybrid workplace

If properly implemented, hybrid environments can improve employee productivity and happiness. The best way to ensure your company reaps the benefits of a hybrid work model is to leverage your technology stack. The efficiency of your hybrid work environment will be determined by how you utilize existing technology and the additions you make to it.

This requires IT teams to adapt user-supporting processes and partner with HR on policies and approaches that support new work habits and work culture. Consequently, IT will have to reprioritize its technology investments.

Here are eight ways to utilize your technology stack to create a dream hybrid environment that your employees will love.

1. Employees should be treated as IT partners

The on-site office system involved the IT team and the CIOs making all decisions about IT. Employees had little involvement with it, and any hiccups they encountered could be resolved by walking up to the friendly tech support staff. Implementing hybrid environments successfully will require re-engineering the IT infrastructure and policies.

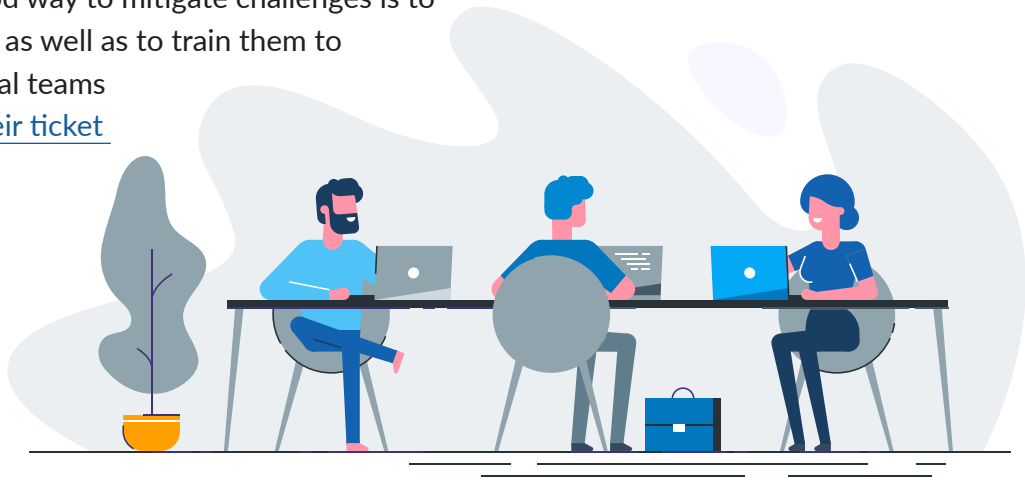
The IT department can give employees a voice in decision making and make them partners in everything from selecting, deploying and improving new technological tools. Employee feedback integrated into a hybrid structure will lead to a better company experience, which will translate to higher employee satisfaction and improved productivity. In these competitive times, where employees expect better work-life balance from their employers, the move is likely to reduce employee churn.

While creating a secure environment for remote workers is a given, IT teams must rethink how they support in-office workers. In the absence of a centralized system, employees need to be able to switch easily from home to the office with minimal friction. The IT teams also need to design their infrastructure to cope with a fluid office environment. In a hybrid environment, real-estate must cater to a wide range of possibilities, including, ranging from a few people in the office to a full house. The IT team needs to plan for both scenarios and ensure that service remains uninterrupted.

2. Provide training and comprehensive support to users

In a hybrid environment, getting a laptop fixed or resolving a network issue won't be as straightforward as heading to your favorite techie's seat. It's always easier to get support when you're in the office, but getting or providing support remotely is harder. Fortunately, most IT teams have a system in place that allows them to offer robust support to their employees remotely since 2020. All they must do is apply some of the best practices to hybrid work culture and make improvements to it.

But that doesn't mean unforeseen challenges won't arise. A good way to mitigate challenges is to work with the various departments and understand their needs as well as to train them to handle simple IT issues independently. By empowering individual teams with the ability to self-support, IT teams cannot only reduce their ticket management workload but also devote more time to business-critical tasks.



3. Adopt scalability and automation

Historically, IT has always been considered a cost, but the pandemic has taught everyone that it is an investment and a necessary one. Although many businesses still use their legacy systems to save costs, this slows productivity and hampers competitiveness at the same time. It is important for companies still using legacy systems to adopt new technologies like cloud and automation so that they can streamline their work and integrate software and tools that'll enable them to save money.

With automated processes, companies can reclaim time from their busy schedules so that they can concentrate on revenue-generating tasks. Businesses are required to perform several mundane repetitive tasks that don't produce revenue but are critical to ensuring their survival. The automation of these tasks will not only free up your talent for more valuable activities but also improve the accuracy with which mundane tasks are completed. The result is long-term cost savings, better accuracy and more time to pursue business growth activities.

4. Restructure equipment policies

One technique that helped employees work remotely was to use their personal devices. Thus, onboarding could be carried out smoothly and employees could start working right away. Many employees preferred to use their own devices due to their superior configuration and familiarity with them, which in turn made their work easier and increased their productivity.

The bring-your-own-device (BYOD) practice not only reduces hardware costs for the company but also encourages employees to take care of their devices. Additionally, it gives employees greater mobility, which increases their satisfaction and productivity. Ultimately, this has a positive effect on the company's financial well-being as well.

As part of a hybrid work culture, employers are also trying to adopt BYOD policies. To ensure that these policies do not compromise the company's IT environment, regulations such as password policies, the use of security solutions, and rules regarding prohibited websites and applications must be clearly defined. Considering that employees use multiple devices nowadays, it is important to set rules regarding the types and models of devices that can be used. The latest cybersecurity tools may not be compatible with old or obsolete devices, which poses a security risk to organizations. Hybrid IT policies should define what employees are required to do to maintain device security.

Download our comprehensive guide to BYOD to gain a detailed understanding of BYOD policies, security risks, benefits and best practices.

5. Restructure the corporate access schedule

Among the results of hybrid work will be time-slice work hours, where employees will work in slices throughout the day, interspersed with personal time instead of working for 8-9 hours at a stretch. While it facilitates a better work-life balance, companies must work out for themselves how to find a common working time for the entire day. This is also known as flexible work scheduling.

The companies determine a few hours during the day when the entire team must work together, but the rest of the working hours are determined by the employees. In this case, IT is responsible for ensuring uninterrupted access to the company network around the clock and providing 24/7 support. Because data is being shared over the company's network throughout the day rather than during peak hours, the IT team also needs to make sure security is constantly monitored.

It is therefore imperative companies invest in a comprehensive cybersecurity program that is also compliant with regulation and government rules. After all, a hybrid work environment's success directly correlates with its cybersecurity provision.

6. Develop and optimize cybersecurity policies

The importance of cybersecurity cannot be stated enough, especially after the surging security issues in the pandemic era. With the introduction of a hybrid environment, the surface area for attackers expands and a decentralized IT increases the risk of an incident or a breach. It's well known that it is easier to prevent a cyberattack than fix it. In 2021, a data breach cost an average of $4.24 million, up 10% from $3.86 million in 2020 — the highest percentage increase year-over-year in the past 17 years.

To keep your hybrid environment secure, invest in the latest cybersecurity tools and systems and take the help of experts to design a system that's right for your business needs, clients and employees. As hackers and threat actors become increasingly sophisticated, so too must CIOs. IBM's 2021 Cost of Data Breach report found that costs of breaches were significantly lower for some companies with a more mature security posture and higher for companies lagging in areas such as security AI and automation, zero-trust and cloud security.

Many corporate cyberattacks are said to be the result of human factor. For organizational security to be strengthened, a "zero trust" approach should be implemented. The Zero Trust Network Access (ZTNA) policy dictates what a user can access. The separation of applications in this architecture allows administrators to set access permissions at a very granular level. At the endpoint front, multifactor authentication should already be commonplace.

As a final precaution, ensure that you have anti-phishing training and security awareness programs to help your employees become the first line of defense against cyberattacks.

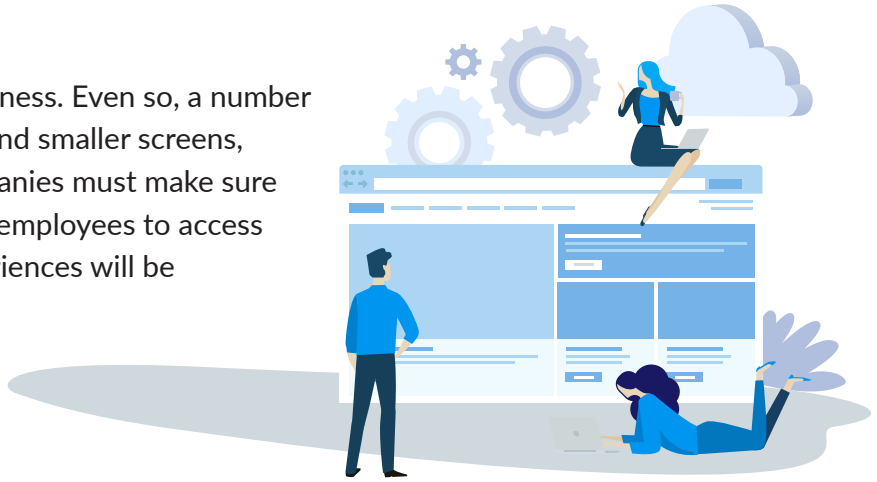
7. Take advantage of cloud computing

The world is moving to trends like big data, automation and mobility that sync seamlessly with cloud technologies. To experience efficiencies, cost benefits and competitive advantage, you need cloud technologies in your workplace. Additionally, cloud technologies can help improve the efficiency of your hybrid work environment since they enable employees to access work-related tools and software as well as share their work with their team members from anywhere and at any time.

Cloud computing will have a positive impact on all businesses. It'll not only help improve process efficiencies but will also allow you to better serve your customers and win more business. This will result in higher revenue and profits. With regard to the hybrid environment, IT teams should ensure that they implement a cohesive cloud strategy in all areas.

8. Implement a mobile-first strategy

Mobile devices are integral to the way clients and employees conduct business. Even so, a number of applications and tools are not optimized for mobile operating systems and smaller screens, whether they are homegrown or provided by vendors. On this front, companies must make sure that all critical business applications can be accessed via mobile to enable employees to access any application or data from their mobile devices. In this way, hybrid experiences will be seamless for employees on the move.



Manage your hybrid workforce with Kaseya

Kaseya VSA is designed to scale with your business. A single SaaS instance of VSA supports tens of thousands of endpoints. Check out how Kaseya VSA can help you manage your hybrid work environment effectively.

Manage all devices

Kaseya VSA is a leading uRMM solution that will give you the capability to manage all devices and across all environments. A unified endpoint management or uRMM solution helps manage all devices, including desktops, laptops and servers, as well as virtual machines and mobile devices. In addition to managing on-prem, cloud and hybrid IT, the tool can manage WFH environments.

Kaseya VSA offers two remote management functions — Live Connect and Remote Control. Technicians can use Live Connect to resolve issues behind the scenes without affecting end users. Remote Control provides both shared and private console access to an endpoint. It enables technicians to access an endpoint with one click, without having to know or manage the target machine's password.

Automation

A VSA feature that will help you with hybrid transformation is automation. Increase productivity of IT professionals by automating routine maintenance tasks with the Kaseya IT Automation Exchange tool. To improve IT security and efficiency, leverage IT processes like software deployment, patch management, weekly maintenance and compliance reporting, and much more. You can also automate remediation of IT incidents to provide your company with an extra layer of security.

Workflow integrations

Kaseya's IT Complete suite of IT management solutions places a strong emphasis on seamless workflows. With workflow integration across RMM, PSA/service desk, IT documentation, backup and disaster recovery, and security, IT operations run more efficiently and operating costs are reduced. In turn, managed service providers (MSPs) can boost profitability and internal IT teams can stretch their IT budgets.

Are you ready to move your business to a hybrid environment? Get a free VSA demo today!

About Kaseya

Kaseya® is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, automate and backup IT. Kaseya IT Complete is the most comprehensive, integrated IT management platform comprised of industry leading solutions from Kaseya, Unitrends, Rapidfire Tools, Spanning Cloud Apps, IT Glue and ID Agent. The platform empowers businesses to: command all of IT centrally; easily manage remote and distributed environments; simplify backup and disaster recovery; safeguard against cybersecurity attacks; effectively manage compliance and network assets; streamline IT documentation; and automate across IT management functions. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.

11302021