Deloitte.

Adaptive Workplaces and Technology

Infrastructure Considerations to Support the Workforce post-COVID

Doug Bourgeois, Alex Braier, Matt Garrett

MAKING AN IMPACT THAT MATTERS *since* 1845

Introduction

COVID-19 expedited changes that many predicted would happen over decades, forcing those seemingly distant changes to happen within weeks. Overnight, the government sector was forced to shift to a telework model and rethink the deep-rooted orthodoxies about how and where work is done. This forced shift towards a distributed and highly virtualized work environment is demonstrating that people can accomplish work efficiently, effectively, and comfortably even while working virtually.

In the United States, almost 60% of employees are now working remotely full or part time and about two-thirds of employees who have been working remotely would like to continue to do so, according to a Gallup poll[1]. Although initially challenging, COVID-19 has presented a unique opportunity for government agencies to reassess where their organizations are headed and proactively shape the future for their agencies and prepare for the long-term. While some agencies will return to a co-located model or reopen the office for a partial return, others have announced plans to stay remote into 2021 and far beyond. Within the private sector, several organizations such as Slack, Facebook, Google and Twitter have announced plans to stay virtual even after the pandemic eliminates the need[2][2]. It is now time for government agencies to similarly identify and prepare for what they will need to enable their workforce in the future.

The decision has moved beyond the traditional binary choice of onsite or telework. Further value can come from **adaptive workplaces.** Agencies can change the way the workplace looks by enabling its workforce to do their work wherever they feel most productive and engaged. This human-centered approach to the workplace promotes productivity, efficiency, effectiveness, workforce well-being and a positive workforce experience. Now more than ever, it is critical for organizations to understand how to create meaningful experiences that connect the work back to the impact it has on employees, users, and customers in achieving their aspirations. Organization are long overdue in developing more adaptive in person and remote workplaces.

Adaptive Workplaces and the Employee Experience

Organizations are uniquely positioned to expand their definition of the workplace to include adaptive workplaces that support the notion that people, and teams, should work where they are most productive, engaged, and inspired, depending on the task and the people. Still – for many organizations – configuring their telework environment remains a challenge. Employees continue to need support from their organizations to understand their policies, resources, and work shifts that have resulted from shifting to full or part-time telework.

Organizations that anticipate working in a telework intensive environment for the foreseeable future should assess and address the six components of the Adaptive Workplace – Mobility Assessment, Workplace Optimization, Productivity and Performance, Connectivity and Well-Being, Facilities Optimization, and Virtual Collaboration, as well as Security

[1] https://news.gallup.com/poll/321800/covid-remote-work-update.aspx

[2] https://www.cnn.com/2020/05/22/tech/work-from-home-companies/index.htm

considerations. Virtual collaboration tools sit at the nexus of these components, enabling productivity and clear communication through secure software that allows for work to get done from home or elsewhere.

Productivity in a virtual environment is highly influenced by and dependent upon the effectiveness of technology and collaboration tools. Some questions organizational leaders may be asking themselves and their employees as they reflect on their virtual collaboration suite include:

- How has the level of productivity changed since telework began?
- What have been the biggest obstacles and challenges staff have faced in carrying out their work responsibilities virtually?
- Does the organization have the necessary IT infrastructure/architecture in place (e.g., servers, networks and platforms) to support a virtual operating environment?
- What virtual collaboration tools are relied on most heavily to perform the work? What challenges does the workforce face when using these tools?

Answering these questions will help agency leaders and team managers understand if their people are teleworking effectively.

While the idea of virtual work, telework, and remote work appear as stretch options for government agencies, it was successfully implemented prior to COVID-19 in several agencies. One such example can be seen at the US Patent and Trademark Office, where the telework program was first initiated in 1997! Since then, the USPTO's Telework Program has grown to be award-winning, with the agency measuring success in terms of its real-estate savings, employee productivity and quality, impact on transit subsidy, employee and customer satisfaction, lower employee attrition and impact on sick leave. David Kappos, former undersecretary of Commerce for Intellectual Property and director of USPTO, said "The USPTO telework programs directly affect our ability to recruit and retain a highly skilled workforce, align examination capacity with incoming workloads, maintain pendency metrics within acceptable limits, and have provided the unintended benefit of helping us reach our goals in domestic and education outreach, knowledge enhancement, and capacity building"[3].

While there are six dimensions of telework, the basis of any telework optimization project, or for that matter, telework enablement, begins with the tools and technology that make it possible. For organizations that recognize virtual collaboration tools and technology as a focus area, effective technical architectures will be a critical aspect that allows for work to occur virtually.

Virtual Collaboration Tools and Technology

To support the shift towards adaptive workplaces, organizations will need to identify and implement changes not just to their people and policy practices, but to the technology which can help enable those changes. Before diving into example solutions, it's important to first understand several of the key technology challenges that organizations shifting to adaptive workplace models face.

Technology Challenges Faced by Organizations Moving to Adaptive Workplace Models

Having an increasing number of users remotely accessing their organizations resources introduces technology challenges that need to be addressed.

[3] https://www.td.org/magazines/the-public-manager/teleworking-thrives-at-us-patent-and-trademark-office

- **Security** – While traditionally, organizations had control of securing their own network, and access to their network resources through on-site devices managed by their IT department, an increasing remote workforce leads to additional security questions and considerations.
  - Are users provided company issued devices, or are they leveraging personal devices? In either case, how are these devices centrally managed and secured?
  - How and where is sensitive data stored and managed?
  - Is traffic encrypted when remotely accessing network resources?
  - How are security policies enforced, such as requiring users to have the latest security updates installed before allowing them access to your organizations network?
  - How can organizations be sure devices aren't compromised and that only authorized users are accessing network resources?
  - How is access and authorization handled across vendors and tools, such as through a federated Identity and Access Management (IAM) system?
  - What features such as Single Sign On (SSO) or Multifactor Authentication are being used to simplify the security experience?

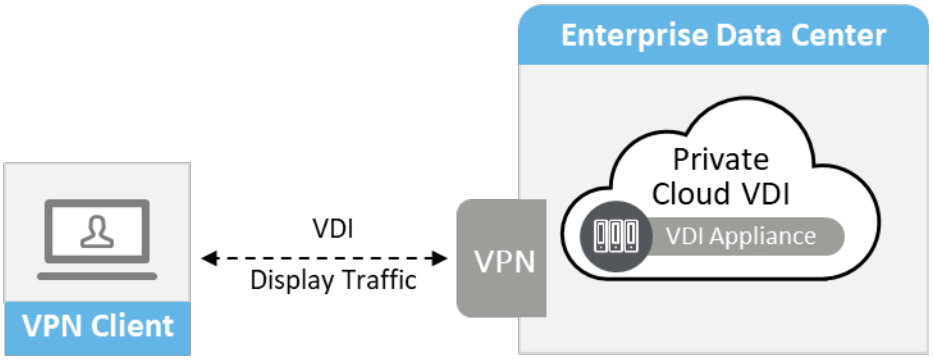
- **Infrastructure** – Users can leverage multiple devices to access their organization's resources and perform work. Depending on the particular user role, devices including phones, tablets, laptops, and VDI will need to be deployed and managed.
- **IT Operations Support** – Technology changes required to enable a remote workforce leads to challenges in providing users with support they may require. Additionally, traditional processes of providing support, such as walk-up IT helpdesk, need to be re-engineered to enable remote support.
  - **Troubleshooting** – New technology, and an increased number of users leveraging technology in new ways to enable remote work, leads to new or previously uncommon problems to troubleshoot. As a result, Knowledge Articles, FAQs, and Best-Known Methods, for triaging issues may not be available, and IT support personnel may require additional training.
  - **Remote Helpdesk** – Providing increased remote support to users may require remote access to devices. Compatibility issues, remote login tool licenses, and connectivity challenges can lead to both operational and cost challenges.

Technology Architectures to Address Adaptive Workplace Challenges

While an adaptive workplace model introduces challenges, leveraging the right technology architecture and tools can help organizations address and get ahead of the increasing number of remote users. The following sections provide potential architectures, while considering both the advantages and disadvantages of each.

Device as a Terminal

Given that a large portion of the workforce owns personal laptops or desktops, taking an approach where users can leverage their existing personal devices as a means of accessing remote or Virtual Desktops Infrastructure (VDI) hosted in their organizations on premise or Cloud Service Provider's (CSP) datacenter can be a valid solution. VDI uses virtual



machines (VM's) hosted on physical servers which is achieved through hypervisor technology, to create virtualized desktop instances on remote centralized servers, which end users can access. By taking this approach, users are provided a very similar experience of using devices on-site with all the same applications, tools, site and network resource access, etc. that they are used to. Organizations also benefit by being able to centrally manage their computers with the same policies administered on physical on-site laptops/desktops. An ideal use case for implementing VDI is for organizations who do not issue devices to their employees, or issue devices to only a limited number of this workforce, as well as an organization with an external contractor workforce.

Benefits of Device as a Terminal to Access VDI

VDI provides several key benefits for a dispersed workforce:

- **Bring Your Own Device (BYOD)** - Employees can use their own devices regardless of the device type, and they do not require robust computing power. As long as they have an active connection to the internet, they can connect to their VDI instance.
- **Familiar User Experience** - The user experience is very familiar and similar to what they experienced when they were in the office sitting in front of a company issued laptop or desktop directly connected to their organizations network.
- **Easier Device Management** - Centralized management of all computers including deployment, maintenance, patching, image deployment, and access.
- **Security** - Increased security as no work is performed locally on devices, and data is stored in locations the organization is able to manage and protect, reducing data leakage. Additionally, VDI reduces the introduction of threats such as viruses being transferred from a personal device to the enterprise network.
- **Scalability** - Ability to scale VDI instances and resources to meet the needs of the organization, particularly when built within a CSP environment, including deploying instances to perform specific tasks that require additional compute power. It is worth noting that costs need to be closely monitored when scaling resources to avoid significant unplanned expenses.

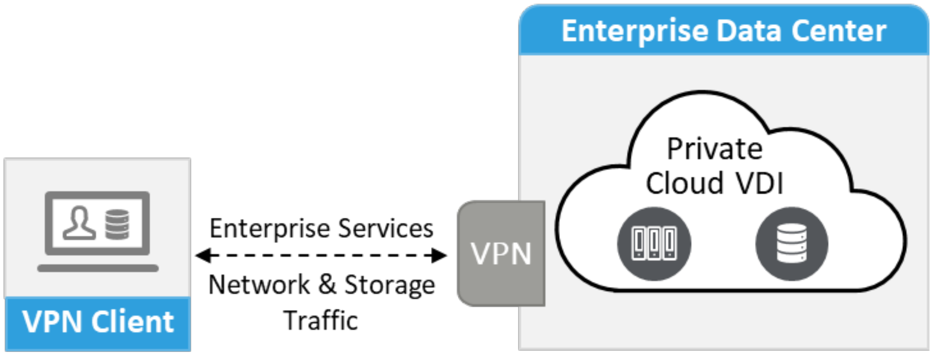
Disadvantages of Device as a Terminal to Access VDI

While there are clear benefits to using VDI, it is not always the optimal solution.

- **Bandwidth Constraints** can quickly become a challenge adversely affecting the performance and experience of end users. Popular remote work applications such as videoconferencing are known to have performance issues and can be challenging to implement with efficiency. Additionally, the end user experience will be subject to their network stability and bandwidth limits, which vary from person to person. Productivity can be negatively affected when performance takes a hit.
- **Complex Architecture** - There is complexity to architecting a VDI environment, which requires expertise to securely and cost effectively plan, size, and build out the solution. Hardware, network, and software licenses needed to build out your VDI environment can also drive up the cost.
- **Outages -** Outages lead to work stoppage. Because user devices are used purely to connect to VDI, and not used to perform any work-related activities locally, if the VDI environment is experiencing issues, user productivity can be brought to a halt.

Device as part of Internal Network

While VDI is a great option where users can take a Bring Your Own Device approach and computers can be centrally managed, establishing virtual private networks (VPN's) to allow your workforce to remotely connect to your organizations enterprise data center, whether it be hosted in a private or public cloud, through issued or personal computers is another possible path to take. Through this approach, a local application is used to connect to and establish a secure connection to the enterprise network and its resources, thereby rendering the user's computer as an extension of the network. This approach is typically used when organizations issue devices to their workforce so that they can manage and enforce policies and updates to reduce security and operational risks.



Benefits of Device as part of Internal Network

- **Familiar User Experience** - The user experience is greater than leveraging VDI, as users are working directly off their local machine reducing performance or network connectivity issues that can impede their work progress and experience.
- **Ubiquitous Technology** - Computers issued by an organization likely already have VPN implemented to allow their users to connect when not on site. As a result, users are already well equipped and setup to remotely access their organizations network in an adaptive environment.
- **Outage Resilient** - Outages or connectivity issues don't necessarily result in work stoppage. As long as users have locally saved their work (ex. in progress Excel or Word document updates) and don't require access to network resources, they can continue working while the issues are being addressed.
- **Reduced Cost and Complexity** compared to architecting an implementing a VDI environment. Establishing VPN to add devices as part of the internal network is a common occurrence that in most cases doesn't require uniquely specialized skills to successfully implement and manage. Additionally, there is minimal hardware and recurring overhead costs when compared to VDI.

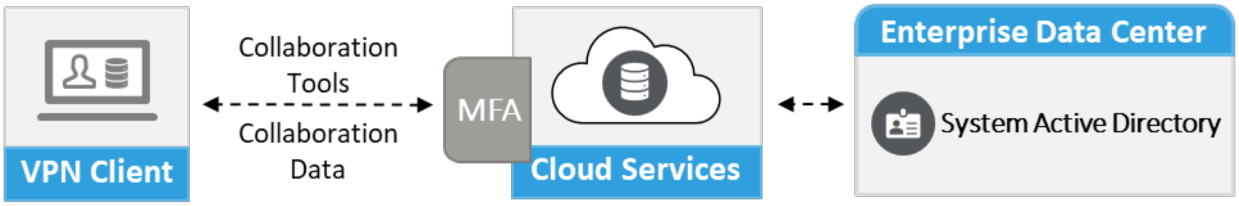
Drawbacks of Device as part of Internal Network

- **Lacking Hardware Requirements** - As devices where work is being performed is local, hardware challenges can arise if devices have incompatibility issues with applications, or if they lack the power to provide a positive user experience. This is particularly an issue when remote users leverage their own devices as opposed to company issued devices that can built and refreshed to meet specifications required for compatibility and performance.
- **Data Security** becomes a factor as users can copy and store files locally, and threats can potentially traverse the network leaving your enterprise resources vulnerable if proper security configurations are not implemented.
- **Identity and Access Management** (IAM) and user authentication becomes increasingly important, both for locally accessing computers, as well as connecting via VPN to the network. Multi-Factor and conditional access needs to be implemented as part of addressing these risks, as well as mature IAM tools and processes.

- **Management of endpoints** becomes a challenge as IT doesn't not have the ability to centrally own and manage all computers like they do with VDI. Managing many different types of endpoints with different operating systems and performance capabilities, can lead to OS configuration and software issues that impact usability.
- **Unanticipated network bandwidth issues** can quickly become apparent as data is sent from the enterprise network to users accessing resources. This can require investment in upgrading network infrastructure and internet service provider costs. Additionally, scalability can become a concern as more and more users are added to the network, bandwidth utilization increases and needs to be addressed.

Device as a portal to services

While Device as a Terminal, and Device as part of Internal Network are means to providing remote users access to resources hosted within an organizations private or public cloud environment, shifting to leveraging Software as a Service (SaaS) tools can help alleviate identified challenges while providing users secure access to critical business applications. For example, migrating to Office 365, Salesforce, Google's GSuite or Amazon Web Services removes the burden of an organization needing to host, manage, and maintain all the infrastructure and applications required to provide users with secure access to business applications and IT management tools such as word processors, payroll, customer relationship management, and endpoint application management software. Pushing that responsibility to a service provider allows users to remotely access resources directly from the providers environment anywhere with any device that has a browser and internet connection. Additionally, with the reduction of in-person interaction, SaaS collaboration tools that can be accessed remotely become increasingly relevant, both for the purpose of staying connected, and to support work collaboration. Example tools include Zoom, Slack, Asana, Microsoft Teams, etc.



Benefits of Device as a Portal to Services

- **Speed of Deployment** - Using SaaS services results in a much quicker deployment than architecting, deploying, and configuring tools within your own data center. In the case of SaaS, the application is already built out and setup in the cloud and requires minimal configuration on the consumers end before usage. Using VMware Workspace ONE as an example, minimal configurations require the addion of domains, users, and endpoint policies while the SaaS provider handles the infrastructure and application deployment and maintenance. With organizations finding themselves thrust into remote work scenarios, leveraging SaaS provides them the fastest and least complex way of providing critical applications to their workforce.
- **Security** (when leveraging mature provider) – SaaS providers are responsible for securing their cloud environments and applications hosted within them. This includes physical sites and infrastructure, virtual infrastructure, network, applications, and data. Leading SaaS providers such as Microsoft, Salesforce, and SAP demonstrate meeting high security standards through holding leading security certifications for their SaaS environments including HIPPA, IRS 1075, SOC1 and SOC2, FedRAMP, ISO 27001, HITRUST, DoD IL2 and DoD IL4, to name a few.
- **Reduced Bandwidth Limits** - Bandwidth limitation concerns are alleviated as traffic is sent directly to the SaaS provider to access applications and does not need to route through your enterprise network. Integration with on premise authentication and authorization services such as Active Directory can still be achieved without adding significant overhead to your network.
- **Reduced Operations and Maintenance** - Application operations and maintenance is offloaded to the SaaS provider, and completely abstracted from the consumer. Activities such as patching, hardware, software, and OS maintenance, and troubleshooting and responding to issues, are handled by the SaaS provider. Additionally, there is little to no downtime

when using SaaS applications due to mature disaster recovery, and high availability architectures which SaaS provides employ.

- **Cost Reduction -** There can be a cost reduction associated with not having to train and deploy staff withing your organization that traditionally owned operations and maintenance responsibilities. Additionally, hardware infrastructure costs are no longer a factor as the SaaS provider owns the environment where the application is hosted.
- **Scalability** – When hosting applications within your private or public cloud environment, scalability becomes a concern as more users are added to your organization who need to access network resources. When subscribing to SaaS applications, considerations such as network and hardware capacity are no longer an issue as SaaS providers are built to scale and accommodate more users as required.

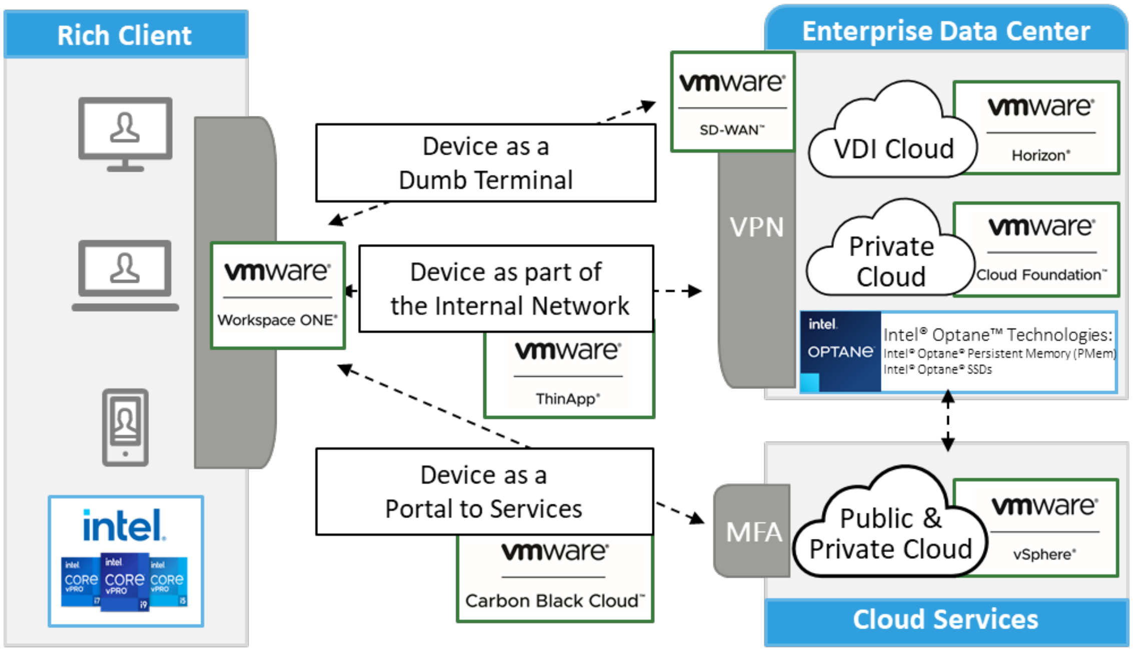
Drawbacks of Device as a portal to services

- **Security** – While mature SaaS providers bring confidence in securing the applications and services they provide, not all providers meet strict security compliance and best practices. It's important to understand what security measures the SaaS provider has in place, what and where data is stored, and how it is protected. Even when leveraging mature SaaS providers, additional security measures for providing user authentication and authorization should be implemented through with the use of IAM tools. Examples include implementing Multi-Factor authentication and integrating with directory services that your organization manages.
- **Migration and Adoption** – Particularly when migrating existing applications to a SaaS model, challenges can arise between customized solutions that were built to meet your organizations business needs, versus what a SaaS service provides. As a result, people and process changes can be required to fit into the SaaS functionality provided. Also, if integration with additional applications or data within your organization is required, there may be limitations or difficulty in integration based on how the SaaS application is developed.
- **Performance** – As users gain access to SaaS applications from anywhere using any device with a browser and internet connection, performance can vary, affecting the user experience. There is dependency on the network the user is connected to when accessing the SaaS service, so there can be challenges in proving a consistent performance experience. Additionally, as SaaS applications are typically accessed via browsers, users who were previously using the application locally on their device (ex. Excel), will likely not experience the same level of performance when remotely accessing the application through a browser.
- **Dependency on provider** – While the burden of operating and maintaining the application and underlying infrastructure is no longer your organization's responsibility, that comes at the cost of depending entirely on the SaaS provider for making sure the applications are secure and available, while having to work within the functionality offered. Solutions that require high levels of customization are likely not going to be a great choice for the migration to a SaaS solution.

Emergence of Integrated Solutions can help alleviate identified challenges with each solution

Regardless of the solution you implement to fit your organizations requirements, there will be challenges that need to be addressed whether implementing new technology, or scaling what currently exists. While these challenges can seem daunting, leveraging leading technology such as VMware and Intel based solutions, can assist in helping to make the transition easier. The examples below provide a view of how VMware and Intel solutions address key challenges identified in each solution.

As described in the sections above, depending on the solution implemented, emerging bottlenecks can arise including VPN Scalability, Bandwidth, hosted services (ex. VDI), and IT Operations/Helpdesk support. However, as seen in the graphic below, VMware and Intel can address issues related to connectivity, data locality & management, scalability, network congestion and security.



The identified tools included in the above graphic work together to provide a comprehensive solution to identified challenges with each approach to enabling a remote workforce. The below section provides a deeper understanding of what the tools provide to accomplish this.[4]

- **Workspace ONE** – A secure digital enterprise platform that delivers and manages any application on any device by integrating access control, Identity, application and multiplatform endpoint management. This offering can be implemented across all devices a workforce uses and serves as a portal to the three modes of operation.
- **Horizon VDI** - Provides a cloud based secure virtual desktop that can be leveraged from any internet connected device. Secure connectivity to the virtual desktop provides users access to corporate applications otherwise not accessible outside the company's infrastructure.
- **VMware Cloud Foundation** – Integrated platform bundling compute, storage, and network virtualization through hyperconverged infrastructure. This supports streamlined delivery of VDI and full stack deployments.
- **VMware SD-WAN** –Supports a resilient, high-performing network infrastructure that uses multiple links and traffic steering technology to rapidly detect downtime or issues, and re-reroute traffic to working pathways. SD-WAN also supports centralized management of the entire network to automate policies for application delivery.
- **VMware SASE Platform** – Cloud-native secure access service edge solution that converges cloud networking and cloud security, combining VMware SD-WAN Gateways, VMware Secure Access, VMware Cloud Web Security and VMware NSX Cloud Firewall into one holistic solution to deliver an optimal and secure cloud application access experience.
- **Carbon Black** – Provides security for all endpoints within your network. This includes anti-virus/malware, threat identification and automated response, security audit trails, and security reporting.
- **Intel Optane** – New class of computer memory & storage that bridges the critical gaps when delivering persistent memory, large memory pools, fast caching and fast storage. When combined with the Intel® Xeon® Scalable processor platform, users can expect to see an increase overall platform performance – even in the most dynamic environments – enabling organization to optimize, store, and move larger, more complicated data sets.

[4] *VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. Intel, the Intel logo, Xeon, and Optane are trademarks of Intel Corporation and/or its subsidiaries in the United States and/or in other countries.*

Where to go from here

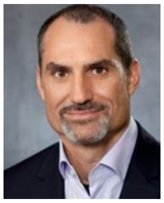
A rapid shift to an adaptive remote workforce requires agility in planning for both the present and future to accommodate this change. While there is a lot to consider, taking an approach of focusing on short term and long-term goals can help reduce the confusion and complexity of where to go from here.

Short Term Goals	Long Term Goals
• Prioritize user access • Educate employees on how to use technology that enables remote work, and security best practices. • Appropriately size for, and increase infrastructure to support remote users • Implement scalable network best practices • Evaluate solutions that meet your organizations requirements and move remote users to leverage VDI, VPN, or a combination • Implement Hyperconverged infrastructure • Support remote Help Desk enablement • Deploy online FAQs, Best Known Methods • Community Contributed, IT Moderated lessons learned • Ticket Management • Increase Automation (RPA, Scripting, etc.) • Secure the remote workforce devices (Rich Client)	• Implement Laptop as a Portal to connect to cloud resources • Decrease VPN traffic by migrating to SaaS solutions (ex. Office 365) • Implement a Multi-Hybrid Cloud architecture • Optimize your cost/capacity equation • Augment IT Operations using AI Chat Bots and implement self-healing and self-service capabilities

Wherever you stand on the telework technology maturity curve, Deloitte can help. Starting with a telework optimization assessment and carrying through to infrastructure design and deployment, Deloitte has years of experience supporting clients on their telework journey. The “new normal” that emerged in 2020 has affected organizations in different ways, and the realities of the new distributed workplace will continue to change. In a paper focused on opportunities, the extreme hardships that the global lockdown brought to many industries must be acknowledged. Deloitte has seen these first-hand and works with clients daily to navigate through the hard times and emerge stronger on the other end. At the same time, this environment does present a rare chance to reimagine where and how we all do business. With that in mind, we are optimistic about the future. Identifying, investing and implementing scalable remote work solutions today is now critical for long-term success. The world has changed and infrastructure that powers our workforce must adapt as well.

Meet the Deloitte Thought Leaders

Key points of contact for any questions regarding the content of this paper.



Doug Bourgeois
Managing Director
Deloitte Consulting LLP
GPS CBO Cloud Engineering

Alex Braier
Managing Director
Deloitte Consulting LLP
Human Capital Org.
Transformation

Matt Garrett
Senior Manager
Deloitte Consulting LLP
Human Capital Org.
Transformation

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.