WHITEPAPER

How to Create Secure, Collaborative and Productive Digital Workspaces

Table of Contents

Abstract

The workplace has changed significantly over the past few years with the rapid adoption of hybrid work. Organizations across all industries can leverage digital workspaces to implement hybrid work models that (1) provide employees with a superior user experience, (2) meet security, productivity and employee satisfaction goals for the business, and (3) are manageable for IT.

This whitepaper explores changing work trends and the various needs of hybrid employees. We will explain what digital workspaces are, the hybrid work challenges they address, how to implement them, as well as use cases and examples of companies that have successfully deployed digital workspaces using HP Anyware.

Introduction

The workplace has fundamentally changed. Rapid adoption of remote work during the pandemic proved that organizations could be successful and employees productive and happy while working outside of the office. But the long-term reality for many companies is that employees aren't working exclusively in offices or at home.

If a workplace is no longer a fixed, physical area, what is it? It's a hybrid workplace, where the goal is enabling employees to work wherever they work best—whether that location is the home, office, event space, client office, construction site, or anywhere with network access in between—and digital workspace technology is pivotal to making it possible.

The adoption of digital workspaces is allowing organizations to be agile and ready to respond to the needs of the business and employees. For IT, this means selecting the right technology that protects corporate assets and centralizes management of corporate intellectual property (IP), while making business information easy to access from devices employees want to use, as well as creating a work experience that's collaborative and has comparable performance to being in the office.

The evolving workplace

Companies across all sectors are embracing the flexibility of hybrid work models. According to the HP Teradici Corporate Cybersecurity Report, 99% of respondents said their companies would continue to offer a blend of in-office and remote working options following the pandemic.

While business leaders see hybrid work as a strategic move for their business, it creates several challenges for IT, chiefly around data security, technology integration and maintenance. It's also critical to get the employee experience right. As HBR noted in an article entitled, In a Hybrid World, Your Tech Defines Employee Experience,

"The technology experiences that employers provide will more or less define the employee experience—technology and workplace tools are, for all intents and purposes, the new workplace."

The way forward is implementing a digital workspace solution that can deliver a high-quality user experience for a wide variety of employee needs and keep business information secure. Digital workspaces closely replicate the on-premises experience when an employee is off-site or at home, so employees can continue to be productive wherever they want to work.

What is a digital workspace?

A digital workspace is a secured, work-from-anywhere, integrated technology framework that can deliver, manage and control centralized company assets, including applications, data and desktops.

Digital workspaces allow employees to access their work in real-time, from anywhere they have a network connection and using any device. It encompasses virtual desktop infrastructure (VDI), data centres, edge, workstations, and applications, whether on-premises or in the cloud, endpoints, collaboration technologies, management and administrative tools, as well as secure access policies and tools.

The virtual nature of digital workspaces makes them highly accessible—corporately managed devices that remain in an office space aren't a requisite to access company data and applications.

When asked about the rise of BYOD—bring your own device—48% of respondents said their companies were encouraging employees to use their own endpoints for work.

A digital workspace that lives on a cloud or on a server stack can be accessible on employee's devices, zero clients and thin clients.

Digital workspaces include collaboration features so employees and peers can work together on the same project—even on the same workspace—when they aren't physically in the same space. They also allow users to share resources. Teams in the same city, or even around the world in different time zones, can leverage shared hosts and applications.

Hybrid work needs are unique

Every company has its own specific needs when it comes to hybrid work, so digital workspaces need to be flexible enough for different types of workers and business needs. Some may require sporadic real time access to very high-performance applications, while others may want to use a specific operating system or peripherals. This could quickly become difficult, even impossible for IT to manage while maintaining security.

Power users and creative professionals

Companies within Broadcasting, Game Development, Manufacturing and Media & Entertainment create and share content that is graphics intensive. They require pixel-perfect re-creations of their content on devices, no matter where they're accessing the data from—the office, home, or another offsite location.

Modern connection management technology offers seamless and low latency access to digital workspaces, no matter where the endpoint or desktop resources are located. Even when highly interactive peripherals, like pens and tablets, are required.

Many of these industries have increased security needs as well, since many work on high-profile projects. With user devices traveling between the office, client or event site and home, or the other way around, keeping files secured within the corporate network is a necessity. For these industries, implementing a digital workspace that only transmits encrypted pixels instead of raw data complies with security requirements, reducing the attack surface, while also eliminating the wait time and frustration of downloading large files.

"Digital workspaces now offer user authentication technologies such as multi-factor authentication (MFA) and federated authentication, which prevent unauthorized access to files and resources, no matter the location of the device gaining access to the workspace."

Due to the variety of devices employees in these sectors use, a unified workspace management system is required so that employees can access data and applications on various endpoints without having to adjust to functional idiosyncrasies introduced by endpoint behaviour. Digital workspaces are designed to give as much access as needed by a user, delivered via their internet connection. IT can also limit access on digital workspaces to certain applications or data, offering more security than VPNs.

Knowledge workers

Knowledge workers in Education, Finance, and Government sectors may not require access to graphics-intensive data, but they still need to have a positive user-experience whether they are working from home or in an office.

For the government and military, security is a high priority especially for disaster recovery and dark site deployments. Similarly for finance and trading businesses, the cost of leaks from cybersecurity hacks could be huge. Interactivity is essential for financial firms where latency could result in transaction delays and loss in profit.

A digital workspace affords knowledge workers a secure virtual environment to work within from anywhere.

Contract workers

Numerous organizations engage contract workers on short or long-term projects. There has been a rising trend in HR to hire based on the best talent available, instead of the location of candidates, which has also seen an increase in the number of contract workers.

Each contract worker may be affiliated with multiple client organizations at the same time. It is inefficient for companies to ship separate devices to these workers—nor would contract workers want several devices to work on. For contract workers, it is better to access various digital workspaces on a single device. And the companies that hire them will have more control over their data security.

How digital workspaces address hybrid challenges

The need for digital workspaces has grown significantly with the adoption of hybrid work models. A variety of endpoints, company-managed and personal, are now accessing company data from numerous locations, which also raises more security concerns for IT.

HP Teradici surveys on hybrid compute security and hybrid work have uncovered common challenges that employees faced when trying to access business information remotely.

1. Security

Keeping business data secure at all times has always been a top priority. Cyberthreats have become more sophisticated over time, and there are many attack surfaces for IT to protect, including more employees remotely accessing company data. One innocent mistake, such as downloading an infected file or clicking an unverified link, could accidentally expose company files to external threats.

Securing the connection to the digital workspace is just as important as securing the enterprise data itself. Digital workspaces allow IT to move beyond Virtual Private Network (VPN) solutions that many companies have traditionally deployed to enable employees to work from home securely.

The HP Teradici security report survey noted that 81% of users found relying on VPNs a challenge due to slow performance and disconnects. The majority of respondents said they were instead actively using remote desktop technology, or digital workspaces.

A digital workspace remotely accessed using PC-over-IP (PCoIP®) technology replaces the need for last mile VPNs while maintaining high security standards. Digital workspaces keep business information safe within your on-prem, cloud or combination infrastructure. PCoIP only transmits information in the form of encrypted pixels, so your data never leaves the data center even while the encrypted display image is travelling from the server to user endpoints.

2. Collaboration

One of the biggest challenges that hybrid workers report is the decrease in 'over-the-shoulder' collaboration opportunities. This is an expected result when teams who used to regularly work together in an office space are working apart, sometimes huge distances away.

Digital workspaces can improve collaboration by offering screen sharing options so team members can join projects and work together in real time. Support for peripherals like USB webcams also enables employees to use a variety of video conferencing apps to remain connected.

3. Varying bandwidth

Businesses have found that even when employees had similar tech and company-issued endpoint devices, available network bandwidth had a major impact on user experience. While working from home, employees found that ease-of-access when remoting in was limited by the strength of their Wi-Fi connections.

Accessing digital workspaces with remote display technology can mitigate Wi-Fi issues as it includes dynamic network adaptation, which automatically tunes to the available network bandwidth without the need for IT to get involved. No matter where employees are working from, and how variable their connections are, access to digital workspaces and resulting workflows aren't interrupted so employees can enjoy an equitable performance.

4. Peripheral device support

Employees can require a variety of peripherals to complete their projects—including webcams, a mouse, keyboards, as well as Wacom pens and tablets for artistic fields.

A barrier to adopting remote work technology has been a lack of peripheral support—when artists are used to drawing scenes with a pen and tablet, it's unreasonable to ask them to switch to another device.

Remote working solutions also often encounter lags between the pen moving on the screen and the actual result appearing. This latency can be extremely disruptive for artists.

"Artists have embraced digital workspaces based on remote display protocols that can stream graphics-intensive content, as well as interactive applications and displays between the host and end-user device."

A remote display protocol overcomes the latency challenge by providing local pointer response cues on a broad range of Wacom Cintiq and Intuos pen displays and tablets, offering artists an accelerated drawing experience and seamless interaction with creative applications independent of distance to the data center.

With lossless color accuracy and low latency while using peripherals, digital workspaces are an efficient solution for artists who need to work from anywhere.

5. Flexibility for IT

IT and employees aren't in the same physical spaces anymore, making remote device management a more crucial aspect of IT's role in a business. The popularity of BYOD has also impacted how IT functions because employees can use personal devices to access business data.

Enterprises now have the freedom to choose between corporate endpoint management solutions or even to allow BYOD, and that has changed the way IT provides support. Digital workspaces can be administered by IT remotely to create secure connections and to manage users.

Deployment methods for digital workspaces

Organizations use a vast array of infrastructure, hardware and operating systems, so digital workspaces are flexible and can be deployed across numerous types of infrastructure, and then accessed from any location with connectivity.

1. Standalone or virtualized workstations

It's important to note that digital workspaces aren't just useful outside of the office. Remote access solutions are designed for physical and virtual workstations to access a centralized source of business data, which can be either on-premises or on the cloud. Once the agent has been installed on the workstation, users can access the digital workspace directly from a Zero Client or Thin Client or they can install a client service on their endpoint device to access their remote machine, data, and applications from anywhere.

2. On-prem data centers

Businesses can also choose to install an agent service on digital workspaces within on-prem data centers and server groups that are privately owned and operated by a business. On-prem data centers can be hosted on private cloud infrastructures, or on physical tower or rack mounted servers in an office space. All employees need for secure workspace access is their own device.

3. Cloud, multicloud, hybrid

Companies that are embracing hybrid environments have found that the cloud is a scalable solution for housing digital workspaces. A cloud infrastructure, either private, public or hybrid, can be accessed by employees working from multiple locations—they can take their work with them without the risks associated with having local applications and data on their endpoint device. While being accessible from anywhere is a benefit, security protocols should be enabled, such as multi-factor authentication (MFA), so that only authorized employees can access business data.

4. Edge technology

As hybrid work has become the norm, more people are now on the go and are increasingly using their mobile phones to access work documents, and even to stream and edit multimedia content. Digital workspaces can be accessed securely using edge technologies on high-speed 3G and 4G networks, as well as 5G portable hubs deployed as hotspots or laptops with in-built 5G capability. With remote display technology automatically tuning according to network available, users can achieve color accuracy and experience minimal latency while working off an edge connection.

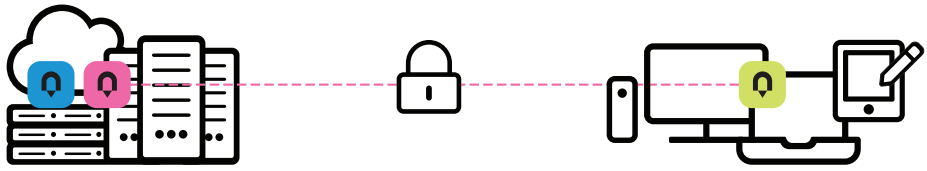
Adding layers of security with digital workspaces

Keeping business information safe, yet making it accessible on a variety of host infrastructures and endpoints, is a high priority for organizations. How can businesses make access to digital workspaces more secure?

1. PCoIP remote display protocol

PCoIP technology has been developed for lossless display reproduction even while using remote endpoints. Additionally, PCoIP traffic is secured using AES 256 encryption, which meets the highest level of security required by governments.

At the server or workstation level, PCoIP encodes, compresses and transmits only image pixels, which are decrypted and decompressed when a user interacts with their digital workspace from an endpoint.



Your corporate data never leaves the server, cloud or workstation but the user still interacts with color-accurate, dynamic and interactive visualization of their workspace from their endpoint.

2. Multi-factor authentication

As businesses move towards Zero Trust adoption and use PCoIP-enabled remote access software, there is another level of security that can help protect data and systems—multi-factor authentication.

While most business data can only be accessed with dedicated credentials, such as a username and password, it simply isn't enough against brute force cybersecurity attacks that can steal and use credentials. MFA adds more levels of verification so potential hackers won't be able to access a digital workspace or endpoint because they won't readily be able to verify their identity.

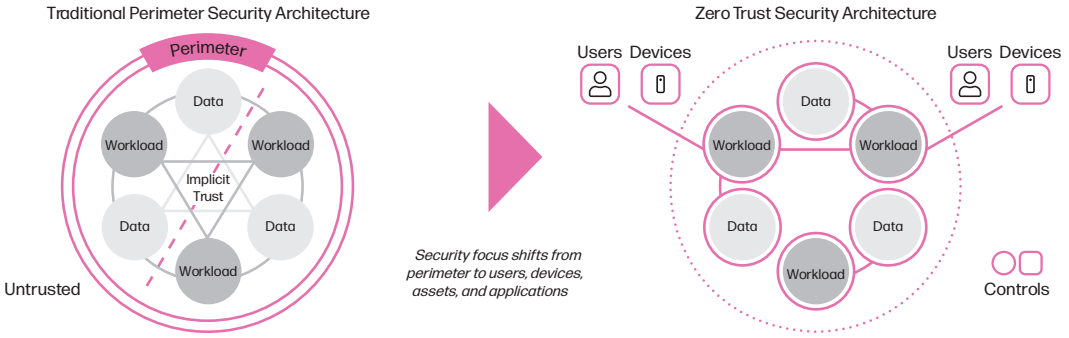
3. IT management

While IT has the ability to manage accounts, being able to manage connectivity to the workspace adds a layer of security for businesses employing hybrid work models. For example, with a digital workspace connection manager, IT teams can use policy-driven decisions to assign workspace resources and manage sessions, thus protecting corporate data from external threats.

4. Zero Trust

Zero Trust is a strategy (and bundle of technologies) that replaces traditional perimeter-based security with a model focused on users, devices, workloads, and data. Users are not provided blanket access to applications, services, and files; they can only access the resources needed for a given task or function. Even within the company network, devices undergo verification and authentication checks at several points before accessing company data.

Extending trust principles beyond mere network access goes a long way to improving enterprise security. By forcing users and devices to authenticate themselves continuously and limiting resource access to only the files and data they need for the given task, users and devices are less vulnerable to hackers.



Best practices for digital workspace success

Your organization may have made the decision to use digital workspaces, but how can you ensure they're effective for IT, employees, managers, and decision makers? Here are a few best practices for digital workspace success.

1. Start with your long-term IT security strategy

IT's strategic role has grown as hybrid work has taken hold. Consulting with IT teams to better understand how security risks and vulnerabilities from employees working outside the corporate offices is a crucial business strategy.

Think of business goals and how they align with the IT strategy.

- What kind of endpoints will be used to connect to digital workspaces?
- Where will employees be working from and what will their performance requirements be?

In large enterprises , the IT team works closely with the Chief Security Officer (CSO) to outline the biggest sources of risk for the company and define the technological and software solutions for mitigating them while ensuring that employees can complete their tasks. IT can also suggest methods for recognizing threats before any leaks occur and for determining the best disaster recovery plan.

Keep communication lines open between management and IT so the company remains aligned on how best to implement digital workspaces and improve operational flexibility during uncertain global conditions.

2. Prioritize user experience

Employee experience should be top of mind when assessing users' technology needs. The success of digital workspaces, and hybrid work in general, depends on making the experience as seamless as possible. Organizations need to know what their employees need in order to work collaboratively and productively, no matter where they are.

- What applications and equipment do they need daily?
- What are the must-haves without which projects cannot be completed?
- What processes could be made easier so that work can be done from different locations?

Managers can take this information to IT teams and start problem solving.

But remember to maintain a balance between needs and deliverables. For IT, security is always going to be a priority but take note of how multiple verification steps impact user experience. Employees will want digital workspaces that offer the highest performance, but resource and network allocations will need to be considered. Strike a balance between employees' needs and IT's concerns by implementing a digital workspace solution that delivers high security and high performance.

3. Create an implementation strategy

A strategy will make it easier to get buy-in from decision makers and to begin the process of implementing digital workspaces. Here are some key steps to consider:

- Establish your budget and build a project roadmap for deadlines and goals
- Create a timeline for onboarding and setting up and activating digital workspace licenses
- Engage with HR on security policies and training
- Determine and track KPIs for digital workspaces

4. Track and improve

Your employees are actively using digital workspaces from a variety of locations; does this mean your work is done? Unfortunately, not. This isn't a one-and-done project.

Track the efficacy of the workspace:

- Is IT comfortable with the levels of security?
- How is the employee experience?
- Are there areas for improvement?
- What new features are available?

Remember, a digital workspace will also need updates—IT will need to update the software regularly, so your organization is using the latest version of the technology.

Digital workspaces KPIs

Service availability (internal)
Determine how often and for what duration digital workspaces were accessed by employees

Service availability (external) Accessibility to digital workspaces for users based on a service-level agreement (SLA) between the vendor and their customer

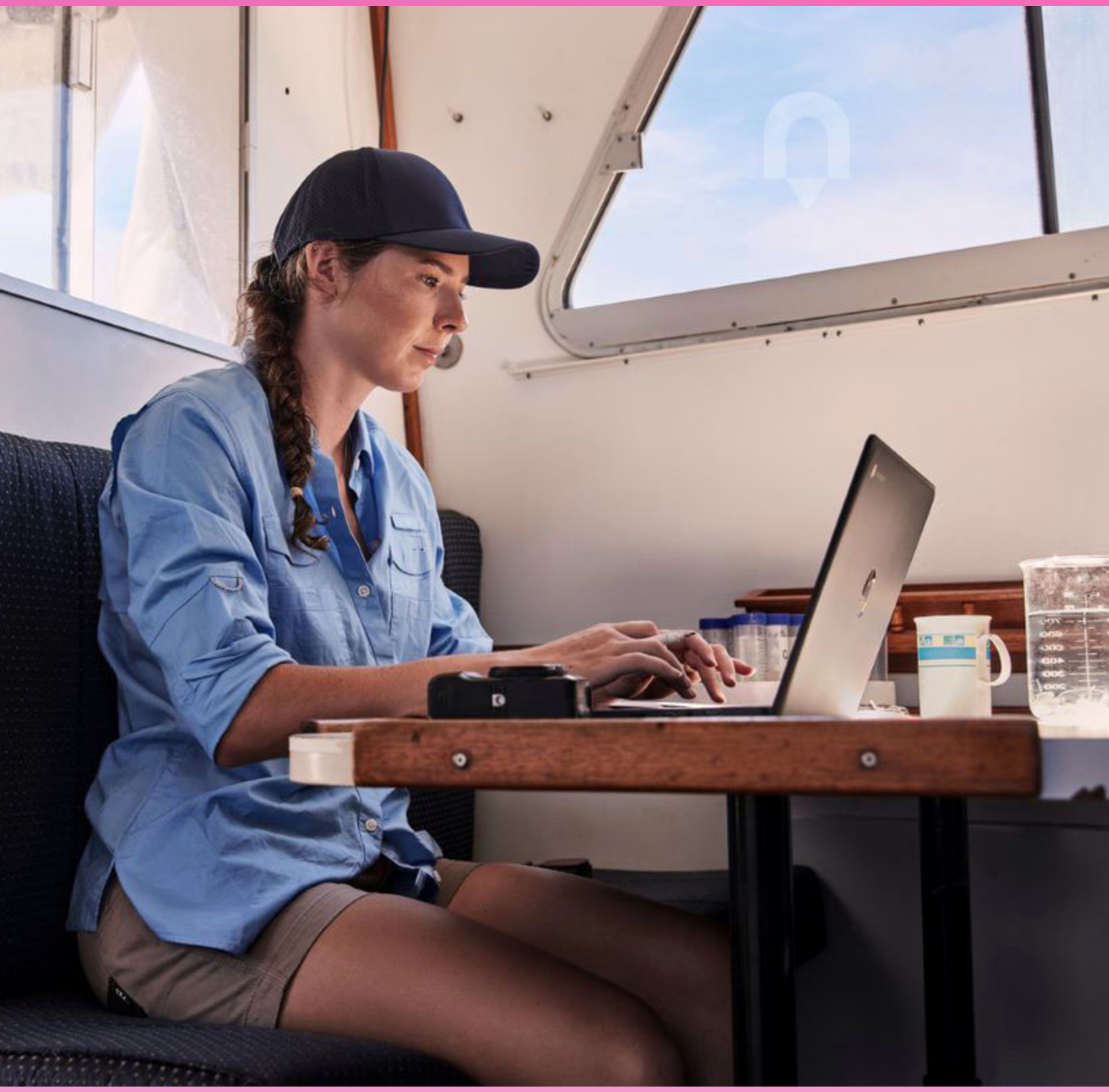
Customer experience
Enterprises that offer downstream digital workspace services of their own should monitor customer satisfaction and churn rates can determine the rate of customer satisfaction or customer churn rate

Employee experience
Ease-of-log-in, responsiveness, access to software, applications and tools, level of productivity and efficiency while using digital workspaces

Resource costs
Calculate the budget variance compared to a baseline without digital workspaces, as well as the cost reductions associated with threat mitigation

Security metrics
Decreased number of security incidents, comparative time needed to detect threats, contain and resolve them, response rates for incidents, number of tickets received and resolved

Digital Workspaces Use Cases



Digital workspaces use cases

1. Disaster recovery

If the pandemic proved anything, it's that businesses need to be prepared for every eventuality. Overnight, companies needed to ensure that employees could take their business data from the office to their home without losing out on security. With a digital workspace, organizations can house their data within a server and give their employees remote access to the required information from their devices. On-prem servers can keep all the information safe and secure while employees use their endpoints to keep working from anywhere.

2. Global economic conditions

There have been significant global changes impacting the way companies function. Medical crises, economic conditions, climate change and rising inflation have led to higher costs for essentials, such as gas and groceries, as well as constraints on the supply chain. Businesses are pivoting to hybrid or remote working models and access to digital workspaces can reduce company expenditures, employee costs, and protect employees from exposure to illnesses, while ensuring employees get the work/life balance that gives them job satisfaction and helps them be more productive.

3. Operating system-agnostic

Personal devices don't always match workstations within the office. When digital workspaces are accessed from devices with a different operating system, the experience is virtually seamless for the user. The host agent transmits the display to the client endpoint regardless of OS—from Windows OS to macOS or Linux, or macOS to Windows OS, and so on—without disruptions to the way the endpoint works.

4. Secure training environments

Digital workspaces can deliver similar types of training environments to a host of employees or students, no matter where they are located or what type of device they are using to attend the training session. With just an internet connection or mobile or tablet connection, a user can remote into a training session hosted on digital workspaces from any endpoint. Additionally, PCoIP has inherent security protocols that ensure training data never leaves the digital workspace environment, so access is protected by multi-factor authentication. The training session will be transmitted via image pixels and no data can be saved on the endpoint device, greatly reducing the chances of a cyber-attack.

5. Convert physical workstations to virtualized workstations

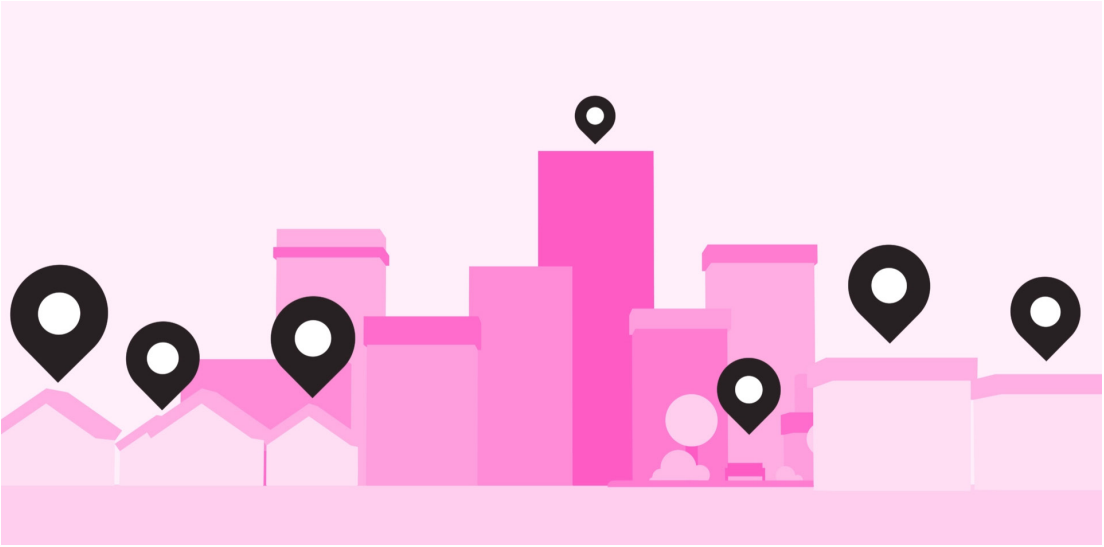
Physical workstations have a space in hybrid work environments. But portability is the most important aspect of working life right now. Employees aren't tied to their physical workstations anymore, just as they aren't confined to working within an office space. By investing in virtual workstations like digital workspaces or providing remote access to the existing inventory of physical workstations, companies can continue to work the way they always did while being mobile.

6. Adoption of public cloud infrastructure

On premises virtual desktop infrastructure (VDI) has long been the popular choice for organizations. But traditional VDI requires CAPEX budget allocation and significant IT management resources, underpinned by a relatively stable headcount. Increasingly organizations are adopting public cloud infrastructure, consumed either as-a-service (such as desktop-as-a-service) or implemented as a hybrid architecture to augment existing self-managed desktops.

Digital workspaces using public could infrastructure have several compelling benefits such as rapid time-to-deployment, shifting expenditures from CAPEX to OPEX, increasing geographic footprint or enabling project-oriented scalability.

Adoption of cloud-centric infrastructure has been accompanied by modernization of authentication schemes too. For example, our security survey shows a shift away from traditional on-prem directory services to the use of federated cloud identity services. Within the next two-three years, 34% of respondents plan to authenticate against a cloud IdP (Okta, Google, or Azure AD) compared to only 17% who will continue to use traditional LDAP authentication services.



Digital Workspaces Success Stories

Atomic Cartoons

Atomic Cartoons is a Vancouver-based artist-driven studio. During the pandemic, the studio had to send over 1000 staff home to work. Employees were in Vancouver and Ottawa, Canada, as well as Los Angeles, United States and were equipped with 10ZiG, LG PCoIP Zero Clients so they could access their Vancouver-based workstations from their personal devices.

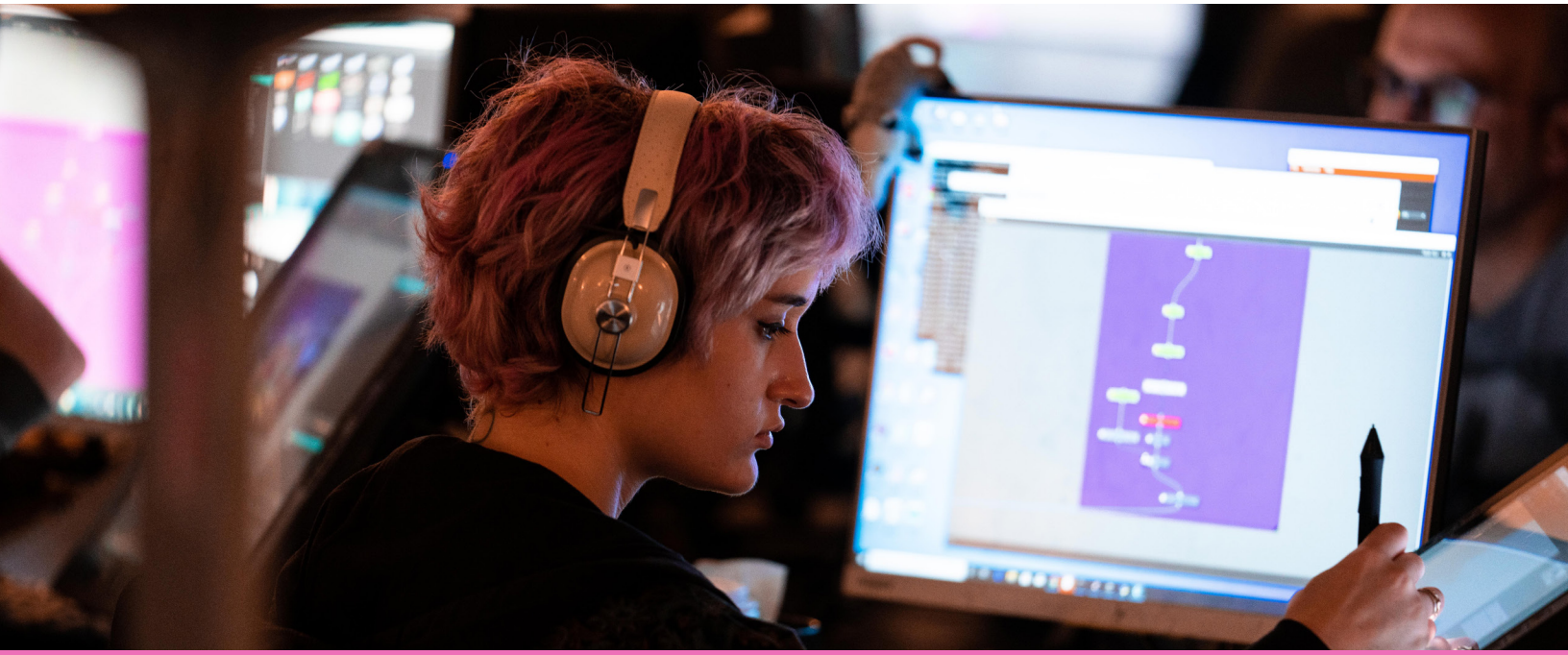
Additionally, Atomic Cartoons had complex compute needs, including access to Wacom pens and tablets, multiple monitors, and graphics-intensive applications.

To centralize their computing systems across locations, Atomic Cartoons turned to HP Anyware, software that they were already testing. In just two weeks, the 13-person IT team was able to onboard the company to HP Anyware.

Security was also a big priority for Atomic Cartoons, since the studio works with IP from major clients such as Disney and Dreamworks. Since PCoIP technology only transmits fully encrypted image pixels instead of raw data, the IP remains safe in the data center.

There was barely any disruption to workflows and not a single deadline was missed. In fact, one of their employees was able to continue working on projects when he visited family in Seoul, South Korea.

The HP Anyware test was so successful for Atomic Cartoons that they found implementing a hybrid work model much easier, after 87% of staff surveyed said they preferred it to working only from home or only in the office. The studio is now looking to expand its employee base beyond North America.



ITV

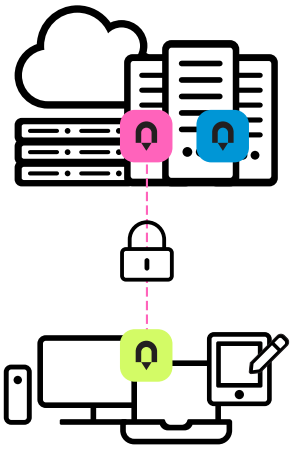
ITV, one of the largest British broadcasters, needed to quickly shift to a Microsoft Azure Cloud environment due to the pandemic. This meant artists, editors, producers, and managers had to work on projects remotely from home.

ITV had already implemented an AVID-based production system, which included three edit suites. What the team needed was remote access to the system through their 10ZiG Zero Clients so post-production teams could continue to deliver on deadline even while employees were working from home.

Initially, ITV used HP Anyware on one project, 10 episodes of John and Lisa's Weekend Kitchen that would be distributed in the UK and another 10 edited for North American audiences. The team were committed to this cloud editing project, finding fixes for issues that cropped up instead of moving back to on-premises work.

What ITV found while using HP Anyware for this editing project was that it afforded teams more flexibility. Without being tied to a physical editing suite, employees could work when and where they wanted while still finishing their tasks. Plus, HP Anyware afforded crisper displays and a dynamic range of color, which made the user experience like working on an on-premise workstation. And the PCoIP environment, that powers HP Anyware, was as accessible on a Mac on a 4G connection as it was on Wi-Fi and LAN.

Not only was the ITV team able to complete editing and distributing the show, but the success of the project has led ITV to adopt a hybrid working model, which will also help the company reach its sustainability goals in the long term.



HP Anyware for Digital Workspaces

HP Anyware* is the enterprise software IT needs to keep people productive with secured access to their digital workspaces. It future proofs against ever-evolving infrastructure, network, and hybrid workforce demands with deployment flexibility for virtually any host environment or workload.

Built on the same technology that won both Teradici and HP an Engineering Emmy® in 2020, HP Anyware creates a seamless experience for teams to interact with their digital workspaces from virtually anywhere.

If you have ever accessed a remote workstation or digital workspace, you have used a remote display protocol. But not all remoting solutions are created equal. Replacing slow and outdated VPN file transfers, HP Anyware leverages the PCoIP protocol to stream highly interactive desktop displays between virtually any host (cloud, data center, edge, workstation) and end-user device (PC, Mac®, laptop, tablet) without any data ever leaving the safety of your network.

Hybrid work is here to stay and with HP Anyware, organizations will be able to access their digital workspaces securely from virtually any infrastructure mix, anywhere.

Connect with a sales representative to find out how digital workspaces and HP Anyware can work for you.

About HP Teradici

HP Teradici is the creator of the PCoIP remote display protocol, which delivers digital workspaces from the data center or public cloud to end users with the highest levels of security, responsiveness, and fidelity. HP Anyware (formerly Teradici CAS), which won an Engineering Emmy® from the Television Academy, powers the most secure remote solutions with unparalleled performance for even the most graphics-intensive applications. HP Teradici technology is trusted by leading media companies, design houses, financial firms and government agencies and is deployed to millions of users worldwide. For more information, visit: www.teradici.com or www.hp.com/anyware.

*Network access required. HP Anyware supports Windows®, Linux® and MacOS® host environments and Window, Linux, MacOS, iOS®, Android®, and Chrome OS® end-user devices. For more on the system requirements for installing HP Anyware, refer to the Admin Guides at: https://docs.teradici.com/find/product/hp-anyware

4AA8-2056ENW, September 2022