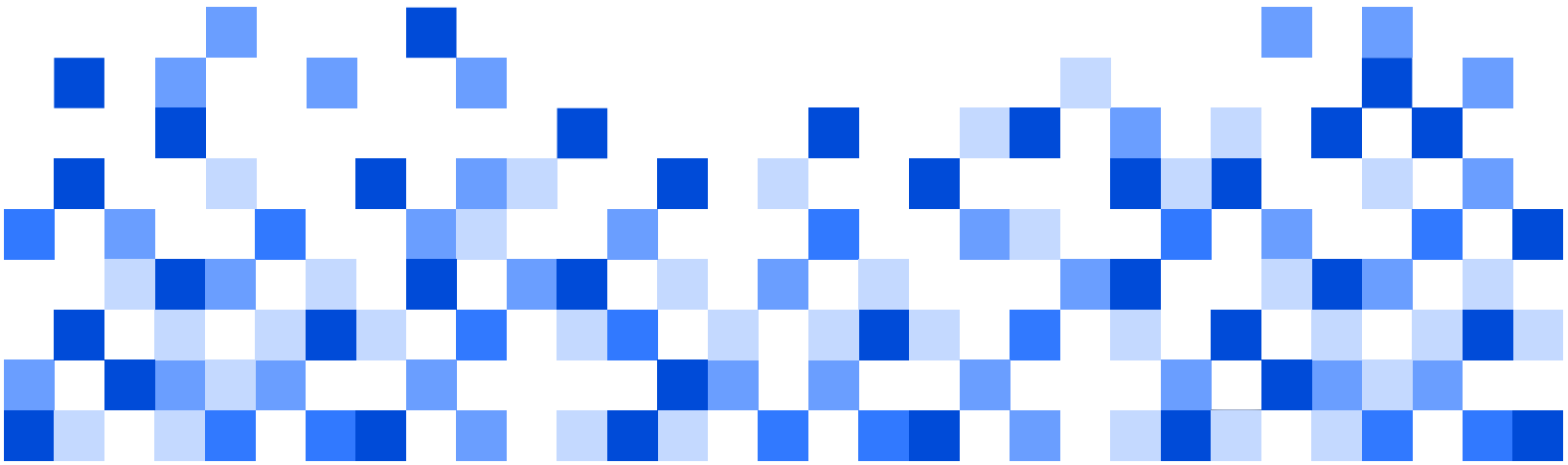
DIGITAL WORKSPACE ECOSYSTEM ALLIANCE

Evaluating the Digital Workspace Ecosystem

A guide to the key technologies enabling secure productivity for the remote & hybrid workforce.



Methodology

To eliminate vendor bias, all members of the Digital Workspace Ecosystem Alliance™ agreed to forego editorial rights to this white paper. The Alliance instead selected Brandon Lee, an independent IT professional with more than two decades of experience with virtualization technologies and author of the well-respected VirtualizationHowTo.com blog to draft this vendor-neutral taxonomy of the Digital Workspace. Alliance members were allowed only one piece of feedback - to confirm or deny the accuracy of their classification in the various layers of the Digital Workspace technology ecosystem. Not all vendors discussed in this white paper are members of the Digital Workspace Ecosystem Alliance, to ensure that key industry players from each layer of the ecosystem - regardless of affiliation with the Alliance - are represented.

Introduction

For most organizations, this past year has required a complete overhaul of how they think, how they operate, and how they enable their people to be productive and secure from anywhere. There's no denying that the pandemic has forced the world to embrace technology in ways never seen before.

Nowhere is this more apparent than in the emergence of the "Digital Workspace." A quick search will reveal that Digital Workspace is a term that has been co-opted by thousands of technology providers, all of which try to define the Digital Workspace in a way that skews the definition towards the particular technology they deliver.

So let's get this out of the way - there is no one singular Digital Workspace solution today.

Today, the Digital Workspace is a framework of technologies that can integrate to help organizations enable their entire workforce - whether remote, in-office, or hybrid - to work productively and securely from anywhere, on any device. And the layered nature of this Digital Workspace ecosystem is actually a feature, not a bug. It enables organizations of any size to identify and select only the technologies that address their particular needs, rather than saddling them with the cost and complexity of many products/capabilities they don't need.

So the million-dollar question becomes - which pieces of the technology ecosystem do YOU need to provide a secure Digital Workspace that meets your organization's and your users' specific needs?

Without a clear understanding of the various components of the Digital Workspace technology ecosystem, that can be a tough question to answer. For this reason, the Digital Workspace Ecosystem Alliance™ has created this guide to understanding and evaluating the Digital Workspace ecosystem. We'll start by providing an overview of each layer, and we'll wrap up with a quick guide on how to self-assess the Digital Workspace tools your organization needs.

The Digital Workspace Ecosystem

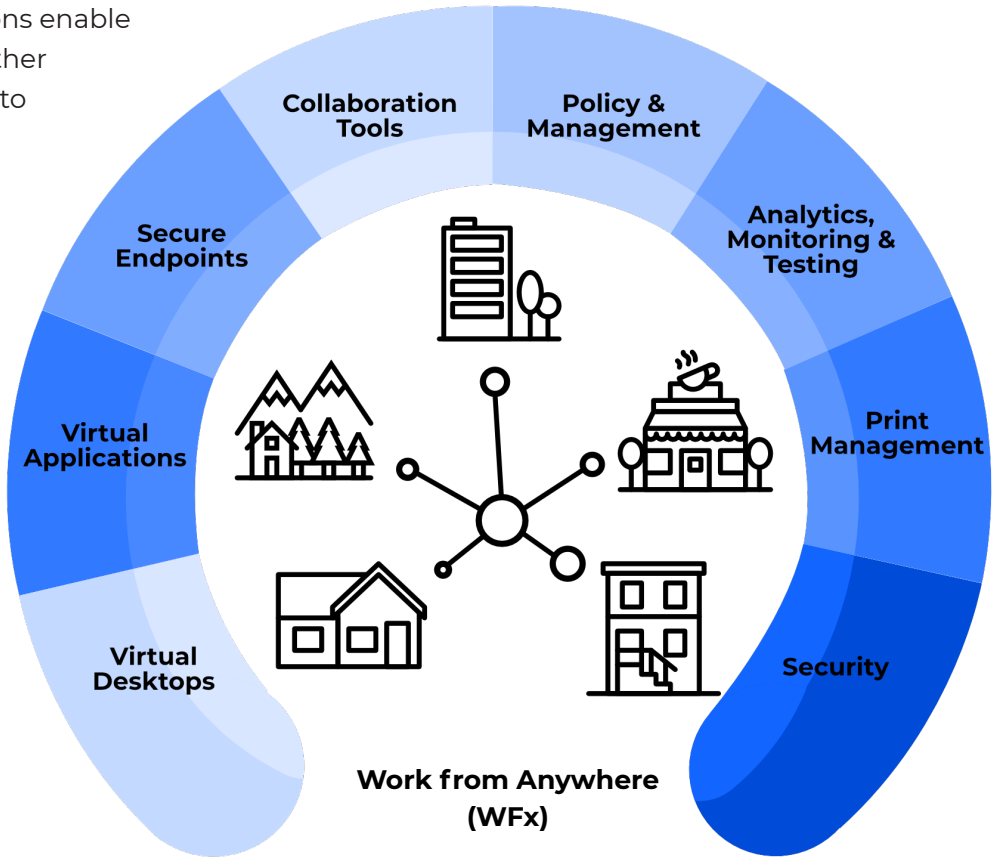


Table of Contents

1 - Virtual Desktops

- How does Virtual Desktop Infrastructure (VDI) work?
- Types of VDI desktops
- Client-based virtual desktops
- Desktop-as-a-Service (DaaS)
- When are virtual desktops a good fit for remote users?

2 - Virtual Applications

- How are Virtual Applications Delivered?
- Benefits of Virtual Application Delivery
- Virtual Application Delivery Use Cases

3 - Secure Endpoints

- Who needs secure endpoints?

4 - Collaboration tools

- What types of collaboration tools are needed?

5 - Policy & Management

- Why Policy & Management tools are essential

6 - Analytics, Monitoring & Testing

- Benefits of analytics & monitoring
- Who needs analytics & monitoring?

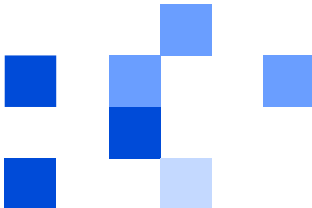
7 - Print Management

- What are print management solutions?
- Who needs print management solutions?

8 - Security

- Why is security so important?
- Implementing secure remote work solutions

9 - Digital Workspace Ecosystem - Self-assessment



1 Virtual Desktops

Virtual desktops have traditionally been one of the more common ways that large organizations deliver Digital Workspace technologies to end-users. Companies provide virtual desktops to remote users in many ways. One of the most common approaches is Virtual Desktop Infrastructure (VDI). VDI technologies have evolved over the past several years from primarily on-premises technology to a solution that stretches from on-premises to cloud and hybrid deployments. Virtual desktops allow businesses to deliver a remote solution with the same look and feel of a physical desktop. Similar to using a desktop in the office, VDI delivers efficient, high-performance access to backend systems and data since the VDI platform is typically housed adjacent to those systems in on-premises data centers.

VDI environments have historically had stringent infrastructure requirements to deliver a reliable and performant environment to remote workers. Due to the sheer number of users and virtual desktops, VDI infrastructure often relies on high-speed backend storage such as modern all-flash or hybrid storage arrays to satisfy the I/O heavy workload demands.

How does Virtual Desktop Infrastructure (VDI) work?

VDI technologies generally work on the premise of delivering pre-configured operating system images and applications utilizing a virtualized environment. VDI abstracts the virtual desktops from the underlying physical hypervisor host very similar to general-purpose virtualized workloads running in virtualized environments. It means the operating system, applications, and data reside on the underlying virtual machine.

Vendor-driven software components allow orchestrating end-user placement to assigned desktops or pools of desktops on which end-users can connect. VDI places users on the "next-available" virtual desktop to service sessions using various brokering technologies.

Virtual desktops are generally accessible via different devices, including workstations, laptops, mobile devices, and others through purpose-built client software. Certain VDI technologies also allow accessing virtual desktops through a web browser as well. Many organizations decide to deploy a thin-client device running a secure Linux OS as a small-footprint device that connects to the on-premises VDI environment.

Types of VDI desktops

Virtual Desktop Infrastructure (VDI) solutions provide three different types of desktops for different use cases - persistent and non-persistent.

Persistent virtual machines are closer to what users are used to when using a dedicated workstation at the office. With a persistent virtual desktop, each virtual desktop is served from a dedicated disk image or virtual machine. All the data, settings, configuration, applications, and the underlying operating system are presented to the end-user exactly where

the user left from the previous session. This type of VDI virtual desktop is better suited for personalization.

Non-persistent virtual desktops are generally the type of virtual desktop presented to end-users in a "pool" of virtual desktop resources. With non-persistent desktops, users are not presented or assigned the same desktop with each connection. Instead, the non-persistent desktop is reset to a pristine state each time a user connects to a new session.

Client-based virtual desktops run as a virtual machine on the remote client, rather than connecting to a virtual desktop housed in the data center. This VM may run inside a VMware Workstation, VMware Fusion, Parallels, or other client-based virtual machine.

Desktop-as-a-Service (DaaS)

With the explosion of cloud infrastructure and services, modern businesses are deploying many technologies "as-a-Service." Virtual desktops are no exception to this trend. With Desktop-as-a-Service (DaaS), a cloud service provider hosts the virtual desktops. They abstract some of the underlying complexity of VDI infrastructure so organizations can consume the service and provide resources to remote users.

Virtual Desktop Use Case

Virtual desktops have specific use cases that fit the technology. As the name implies, virtual "desktops" are excellent for users who need an entire desktop session to carry out business tasks. Power users who need to interact with a full desktop session benefit from VDI-based virtual desktops. These types of users may include developers, graphics artists, engineers, and others.

Users who perform hardware-intensive operations requiring full-desktop session interaction and even GPU-accelerated applications are a prime candidate for virtual desktops. There have been many powerful advancements in VDI technology related to GPU offloading. These use cases often include working with artificial intelligence (AI) and machine learning (ML) applications that offload processing to powerful GPUs installed in the host hypervisor.

However, full virtual desktops are often overkill for most remote users since the majority of people only need to access standard applications from any device to remain productive. Provisioning complete VDI solutions for remote workers who only need to consume standard applications is generally not the most efficient or best fit for virtual desktop technology.

Key Players

Citrix, Microsoft, Nutanix, Tehama, VMware

2 Virtual Applications

Virtual Application Delivery solutions provide an excellent way to simply and securely enable your users to access business-critical applications on any device, regardless of their location. Prior to the pandemic, some companies would utilize full virtual desktops simply to provide their people with remote access to their productivity applications – but cost and performance pressure, as well as security and compliance concerns, have led to an increased demand for alternative solutions.

Virtual Application Delivery allows organizations to eliminate the need to provide virtual desktops to all users for application access. Instead, applications are delivered directly to remote users on any device securely via any HTML5 browser, without the need for a virtual desktop. Many organizations choose to utilize Virtual Application Delivery for all of their users, but it is also often deployed alongside Virtual Desktop solutions. Doing so enables organizations to provide different users with the right level of technology based on their needs.

For example, it's common for large organizations to reserve VDI access for power users who need to interact with a full desktop session, while utilizing Virtual Application Delivery for the remainder of their users who simply need to access their business-critical apps. As the name implies, Virtual Application Delivery focuses on the seamless and straightforward delivery of applications to remote users.

Easy to setup and deploy, Virtual Application Delivery was often seen as an immediate solution for emergency scenarios (such as the pandemic) to provide employees with secure access to business critical applications from outside the secure corporate perimeter. In the long term, Virtual Application Delivery is now becoming a key piece of many organizations' strategy for enabling their people to work from anywhere (WFx) - whether that's fully remote, internal, or hybrid - by enabling the flexibility to securely access desktop and web applications as needed.

How are virtual applications delivered?

With Virtual Application Delivery solutions, Windows applications web apps are delivered to end-users over a simple and secure HTML5 web browser connection. This approach alleviates the need for specialized client software or agents and enables the secure use of both private and corporate devices. Publishing an application or service can be done within minutes by normal administrative personnel - no deep technical expertise required - and users have zero learning curve as they still get to use the same exact version of the apps they've always used - just running in a browser.

Benefits of Virtual Application Delivery

Virtual Application Delivery allows companies to quickly and easily create a modern Digital Workspace for end-users to access business productivity applications. Applications do not have to be retooled, refactored, or relocated. Companies can deliver access to their applications from either on-premises

datacenters, any cloud provider, or hybrid environments.

Another benefit of Virtual Application Delivery is the resource requirements. Compared to delivering an entire desktop session to an end-user, Virtual Application Delivery requires only a fraction of the resources of VDI or DaaS. Since Virtual Application Delivery is significantly leaner from an infrastructure perspective, this reduces the complexity and technology footprint. It translates into cost-savings, less complexity and administration time, reduced maintenance, and a drastically reduced cybersecurity attack surface.

Modern Virtual Application Delivery allows streaming applications, both current and legacy, to end-users. Like Virtual Desktop Infrastructure (VDI), all data stays securely located in the data center, whether on-premises or in the cloud.

Virtual Application Delivery Use Case

Virtual Application Delivery helps organizations solve many complex remote access challenges. It also plays a key role in cloud migration initiatives as it abstracts the underlying infrastructure from the end-user to deliver applications. Many companies find that Virtual Application Delivery makes sense for many, if not most, of their users. Most users do not need to interact with a full virtual desktop but instead only need to consume their business-critical applications.

After examining end-users needs, most businesses find that Virtual Application Delivery is a layer of the Digital Workspace ecosystem that allows meeting the needs of most end-users and creating a much more efficient delivery platform. It reduces the infrastructure needed to deliver those applications and bolsters its overall security profile by reducing the attack surface. Its ease-of-implementation as well as ease-of-use allow instant deployment with close to no user instruction.

Virtual Application Delivery also provides an option for independent software vendors (ISVs) looking to SaaS-enable traditional applications that may not be cloud-ready. Refactoring conventional applications for the cloud may not be possible, financially feasible, or quickly achievable. Organizations who need to promptly shift applications to remote delivery can easily do so using Virtual Application Delivery solutions to deliver any application to any device with just a few simple configuration steps.

Key Players

Cameyo, appCURE, AppStream 2.0, Fortinium, Tehama

3 Secure Endpoints

Security has come into clear focus in every aspect of technology today. Especially since the COVID-19 pandemic began and the tremendous shift to a distributed workforce, many businesses have found it challenging to keep security front and center while providing remote workers with access to business-critical applications.

Conventional applications were generally not designed for off-premises access or with secure access in mind. Many organizations are still using legacy applications to carry out business-critical functions within their environment. It leads to a dangerous combination of weak application security and insecure ways of accessing those traditional applications at the edge. As users are now increasingly located in edge environments, including home networks, securing endpoints and providing secure remote and hybrid work solutions are essential for cybersecurity.

With the threat landscape increasing by the minute and cybercriminals using new and innovative means to attack environments, businesses must give due attention to end-user client security. An additional threat is exfiltration of sensitive corporate data to personal devices with end-users who are allowed to use bring-your-own-device (BYOD) to access corporate environments. How can organizations provide adequate remote access endpoint security? Also, how can they effectively separate personal devices and business-critical data? These crucial objectives can be met using the next layer of the Digital Workspace ecosystem - Secure Endpoints.

Secure endpoints help ensure secure remote access for all of your users. Secure endpoints provide businesses the capability to allow end-users to use BYOD while effectively separating insecure BYOD software environments from business-critical data.

For example, no data is stored on secure endpoints, especially when enabling BYOD. All information is stored in the cloud instead and not in the context of the personal device. Some solutions even provide a cloud-native operating system that can run on almost any hardware platform and provides the ability to provide secure remote endpoints that foster productivity and security.

Secure Endpoints Use Case

Organizations must have a strategy for secure access to business-critical systems in edge environments. While secure endpoints make sense for many verticals, specific industries should pay special attention to secure endpoints for remote users as these industries are generally front and center for cyberattacks. These include:

- Healthcare
- Government
- Finance
- Retail
- Higher Education

According to the IBM Cost of a Data Breach Report 2020, Healthcare incurred the highest average data breach costs for the tenth year in a row at $7.13 million. Cybercriminals specifically target industries with extremely valuable, sensitive, or otherwise useful data they can sell on the dark web.

Secure Endpoints Use Case

IGEL, Neverware, Praim, Stratodesk, Tehama, Wyse

4 Collaboration Tools

A layer of the Digital Workspace ecosystem that has come into clear focus since the beginning of the pandemic is collaboration tools. As organizations have shifted to a distributed workforce where an employee's location is no longer the corporate office, in-person collaboration, meetings, and other daily activities can no longer be carried out by traditional means.

As the pandemic has shown, effective collaboration tools are crucial to maintaining communication between teams, employees and supervisors, and even employees and customers. Collaboration and communication have shifted to all digital platforms, and, as a result, these have seen tremendous growth and widespread adoption.

Collaboration Tools Use Cases

When considering the various collaboration platforms, which platforms appeal to which businesses? Even organizations who may have initially thought digital collaboration tools were not needed most likely have seen the need for these over the past year during lockdown mandates and social distancing regulations. This past year has changed the way employees work and collaborate.

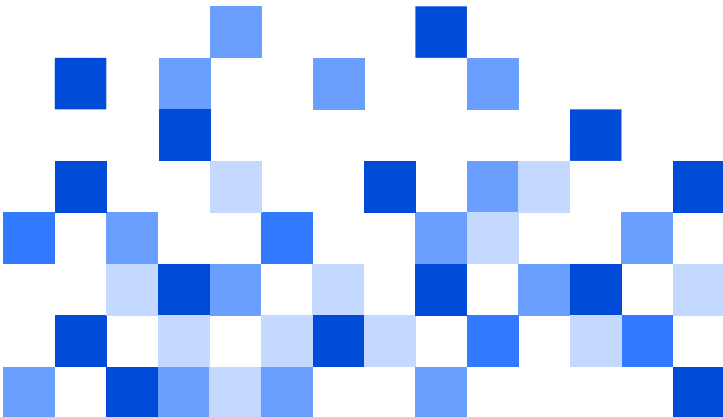
This change underscores the need to provide the proper tools supporting new ways of communicating, securely.

Most likely, the workplace and the way employees work will be changed forever, even post COVID-19. Businesses must have a solid digital collaboration strategy as part of their overall Digital Workspace solution moving forward. Choosing a solution that aligns with current business needs, solutions, and other criteria will be a decision that will no doubt have a different answer for each business. However, there is no question. The Digital Workspace, for most organizations, will include the need for robust digital collaboration tools.

Key Players

Key Players

- **Messaging –** Google, Microsoft, Slack
- **Video conferencing –** Google, Microsoft, Zoom
- **Project collaboration** – Asana, Microsoft, Wrike



5 Policy & Management

Organizations are tasked with many challenges regarding their business-critical data, especially when delivering access to remote workers. These challenges include:

- Security
- Compliance
- Management

With the multitude of security threats to business-critical data and the need to align business processes and practices according to various governance guidelines, policy frameworks are essential. Also, management solutions can monitor, troubleshoot, and maintain the multiple components of the Digital Workspace ecosystem.

Proper management tools automate many of the tasks that would need to be manually carried out otherwise. This includes monitoring the Digital Workspace environment for issues and performance trends, and having the right troubleshooting tools and automated actions to trigger various infrastructure issues.

Also, policy tools provide the means to control end-user activities per business technology policies. Policies provide the guardrails needed to ensure that end-user activities do not introduce security threats in the environment. Businesses today are also subject to many different regulatory frameworks requiring policies for aligning business and end-user activities.

Compliance regulations may include: General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and more.

Managing and securing hybrid remote environments can be challenging because not all management systems were designed for modern management scenarios. Policy management solutions provide the management, security, automation, and reporting tools that can help modernize and extend the power of your existing infrastructure.

Policy & Management Use Cases

Today's very complex and challenging work environments, which may include very distributed, hybrid remote work environments, are increasingly difficult to manage, secure, and bring into compliance. When talking about enabling all of these actions manually, it simply becomes impossible at any scale. Having the right technology tools to manage the layers of the Digital Workspace ecosystem and provide needed controls via policy management is extremely important.

Policies managing Digital Workspace solutions provide protection for business-critical data and end-users against cyberattacks. As compliance demands grow for businesses and data privacy laws are extended, enforcing policy management across the Digital Workspace environment is going to become even more important.

Key Players

ControlUp, PolicyPak, VMware, Microsoft, Tehama

6 Analytics, Monitoring & Testing

Closely related to policy and management tools, analytics, monitoring & testing solutions are crucial tools in any technology ecosystem, including the Digital Workspace ecosystem. Capturing analytics and monitoring data is vital to having visibility to key performance indicators (KPIs) in any Digital Workspace environment. Having key analytics and monitoring data is essential for troubleshooting.

Analytics, monitoring & testing of remote work environments and the components of the Digital Workspace ecosystem should involve capturing performance metrics for:

- Applications
- Logins
- Users activities
- Compute
- Storage
- Networking
- Usage

Benefits of Analytics, Monitoring & Testing

By analyzing performance metrics and monitoring user activities and other KPIs in the Digital Workspace environment, businesses have the tools to ensure a smooth remote & hybrid work experience that does not impact business productivity. It also reduces the time to resolve issues and pinpoint "hot spots" in the environment before becoming more significant.

Analytics, monitoring & testing also helps to understand the overall picture of your Digital Workspace. It can help define a baseline of performance, user activities, and other values, which helps to more quickly understand when there may be an issue with the environment.

Analytics, Monitoring & Testing Use Cases

Analytics and monitoring are crucial components of the Digital Workspace ecosystem. Without capturing performance and usage analytics and monitoring components of the Digital Workspace, businesses are flying blind

when problems arise or issues are reported.

Remote & hybrid work solutions using virtualized desktop environments such as Citrix XenApp, XenDesktop, Microsoft RDS, and VMware Horizon View benefit from the performance insights provided by analytics, monitoring & testing solutions. Monitoring the performance of remote work solutions helps to ensure end-users work efficiently and effectively.

These solutions help businesses monitor and troubleshoot any issues that arise with the underlying virtualized infrastructure backing remote work solutions and hybrid work configurations. They can also allow companies to monitor and gather analytics data on business-critical applications, helping organizations understand KPIs with applications as they provide remote work environments for the distributed workforce.

Key Players

ControlUp, LoginVSI, Tehama, VMware

7 Print Management

Printing remains a business-critical function for many organizations and is key to a smooth user experience in Digital Workspace environments. When deploying remote & hybrid work systems to empower people with the tools and solutions needed to carry out business-critical activities, printing and management of print devices is a vital component of the Digital Workspace ecosystem.

Organizations often find that the built-in printing solutions in Citrix, VMware Horizon, RDSH, and others are less than adequate or lack the centralized management features required for providing robust print solutions for remote users that are manageable and secure.

Print Management solutions provide businesses with the tools needed to securely manage print devices, regardless of the type of endpoint device, in a single management interface. These types of devices include physical and virtual environments such as those used in most Digital Workspaces.

Print Management Use Cases

There is no question that print management is notoriously challenging, expensive, and time-consuming for IT staff who often spend hours managing print devices, drivers, and troubleshooting issues. Legacy printing solutions and challenges can often hinder businesses from making the digital transformation needed for today's modern hybrid workforce. Print management solutions are essential for businesses where the need for printing is a business-critical activity.

For those with business-critical printing needs for both on-premises and remote workers, print management solutions allow organizations to manage their print solutions across the board effectively. With the wide range of devices and environments organizations are using today, print management solutions must deliver effective, efficient printing in a wide range of different remote work solutions. Print management solutions tend to work with any device, including mobile, in any environment.

Key Players

directprint.io, ThinPrint, Tricerat

8 Security

Security is uniquely positioned in the Digital Workspace ecosystem and should be a requirement for every Digital Workspace strategy, as well as comprising an essential layer of the ecosystem in its own right.

There has never been a more urgent need for companies to secure their business-critical data than now. Cyberattacks are at an all-time high. New threats are emerging daily and emphasize security as a top priority in the Digital Workspace ecosystem.

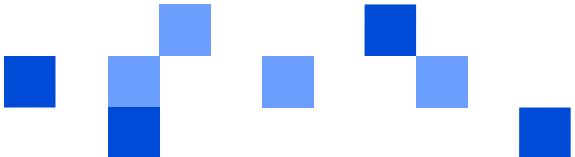
Cybercriminals have been targeting remote workers since the beginning of the pandemic. The Federal Bureau of Investigation (FBI) noted a 400% increase in cyberattacks early on in the pandemic. Ransomware is a favorite tool of highly successful attackers and is increasingly being used to compromise business-critical data. This trend is undoubtedly going to continue. Cybercrime Magazine predicted a ransomware attack on businesses in 2021 every 11 seconds, inflicting $6 trillion in damages.

Many remote & hybrid work environments are riddled with security configuration issues. Organizations hard-pressed to implement solutions quickly, such as at the beginning of the pandemic, may have rapidly implemented remote work solutions not appropriately configured for security.

A classic example of this is using a publicly exposed RDP server without using the recommended RD Gateway configuration as a proxy for RDP traffic. Remote Desktop Protocol (RDP) is notoriously vulnerable, especially in unpatched systems.

Attackers are keen to find environments and remote/hybrid work products where proper security configuration is not implemented. Improper security configuration of Digital Workspace solutions can lead to easy and quick compromise from a cyberattack.

Modern security priorities require security to be intrinsic to the Digital Workspace solutions chosen. It also includes the requirement to secure each component of the Digital Workspace.



Security Use Cases

Choosing remote work solutions with intrinsic security built into the platform allows businesses to deliver the critical components of hybrid remote connectivity and align with security requirements. It is especially true when choosing Digital Workspace solutions for remote employees. Let's look at examples of providing intrinsic security in various remote and hybrid Digital Workspaces solutions.

Within the Virtual Application Delivery layer, it's critical to look for solutions that provide intrinsic layered security built into the platform that enables you to deliver applications while securing data access. Virtual Application Delivery solutions should utilize a Zero Trust security model that eliminates the need for VPNs, only allows network layer connectivity for authenticated users, and be capable of reverting remote environments to a pristine state upon disconnect while preserving business-critical user data to the cloud.

Secure browser technologies enable increased security for remote and hybrid employees without impacting productivity. These virtualized browsers offer a secure environment to access corporate applications and services without using a VPN while also protecting on-premise workers from cyberattacks when accessing the internet.

There are also security tools capable of providing a central context platform enabling companies to let their people work securely from any location, any device, over any network. These empower IT teams with the controls to meet all security, compliance, and regulatory standards.

Key Players

Cameyo, deviceTRUST, Fortinium, Okta, Ping, Tehama, VMware

9 Digital Workspace Ecosystem Self-Assessment

The Digital Workspace ecosystem is a framework of interconnected technologies that allow organizations to enable a productive, secure, and collaborative workforce no matter the location or device. The layered characteristics can help organizations identify the various components of the ecosystem they truly need for their business. Each business use case is different and may require different components of the ecosystem to empower remote and hybrid work effectively, efficiently, and securely.

The brief self-assessment questions that follow can help you narrow things down to

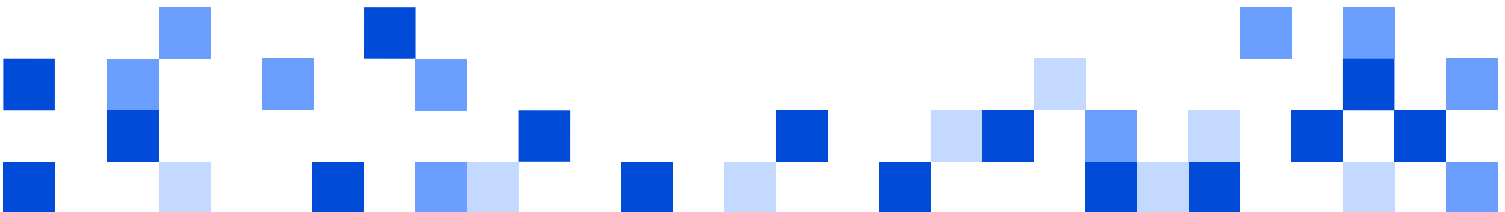
the specific layers of the Digital Workspace ecosystem that fit your business needs and use cases. The needs of each organization will vary, and this is not an exhaustive list of qualifying questions, but it is a good place to start your evaluation of Digital Workspace solutions.

Virtual Desktops	Citrix, Microsoft, Nutanix, Tehama, VMware

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. Power users (engineers, developers, graphics artists) 2. Applications needed require heavy graphics processing power 3. Securing data, so it never leaves the data center	1. Users need access to standard applications 2. There is no need for heavy graphics or other processing power 3. Organizations want to keep the infrastructure, cost, and security footprint to a minimum

Virtual Applications	Cameyo, appCURE, AppStream 2.0, Fortinium, Tehama

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. Users only need to access business-critical applications 2. There is no need for full desktop interaction 3. You want to modernize productivity applications for remote access without redeveloping your apps 4. You want to reduce your attack surface, infrastructure footprint, and management costs	1. Power users that require a full desktop 2. Applications using GPU-accelerated computations are needed, such as in AI and ML applications

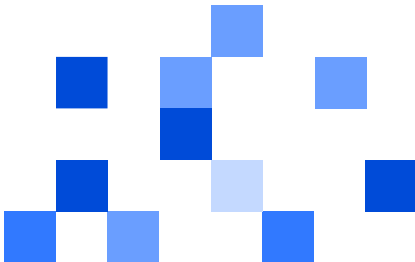


Secure Endpoints	IGEL, Neverware, Praim, Stratodesk, Tehama, Wyse

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. Users may need or be allowed to access business data with BYOD 2. Data is sensitive 3. Industries prone to cyber attack 4. Regulatory and compliance requirements	1. Organizations are already using secured thin clients to access business-critical data 2. Edge locations without cloud connectivity

Collaboration Tools	Google, Microsoft, Slack, Zoom

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. Traditional communication is not possible 2. Providing flexible work solutions to remote employees 3. Empowering workers with more effective and efficient ways to communicate	1. There may be corner cases due to regulatory or other compliance regulations with restricted digital communications 2. There are no security solutions in place to control access, data, and other shared information



Policy & Management	ControlUp, PolicyPak, VMware, Microsoft, Tehama

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. End-user activities need to be controlled in the Digital Workspace ecosystem due to security and/or compliance reasons 2. You want to have the tools needed to troubleshoot and quickly identify infrastructure issues in the Digital Workspace environment 3. You want to reduce the time to resolution for issues	1. There may be corner cases due to regulatory or other compliance regulations with restricted digital communications 2. There are no security solutions in place to control access, data, and other information shared

Analytics, Monitoring & Testing	ControlUp, LoginVSI, Tehama, VMware

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. You need to understand key performance indicators (KPIs) of your applications 2. You want to reduce the time to resolution 3. You need visibility into user activities throughout the Digital Workspace ecosystem	1. An MSP may maintain your Digital Workspace 2. You are using a hosted solution 3. Other layers of the ecosystem may be more important for budget reasons

Print Management	directprint.io, Tricerat, ThinPrint

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. Printing is a business-critical activity 2. You need to manage printing activities across all devices and remote work locations 3. You want to have centralized visibility and management to print devices	1. Physical printing is not an important part of your business process or is not used altogether 2. No physical copies of information are needed (invoices, documents, etc.)

Security	Cameyo, deviceTRUST, Fortinium, Okta, Ping, Tehama, VMware

When is this ecosystem component needed?	When is this ecosystem component not needed?
1. Security should be a top priority in all layers of your business, including all technologies used 2. Reduced cyberattack surface 3. Regulatory and compliance requirements 4. Protecting business-critical data 5. Safeguarding your business from fines, legal action, and tarnished business reputation	1. N/A

v1.0 20210401