

## VDI Challenges for a Secure Remote Workforce



## INTRODUCTION

# Virtual desktop solutions have long been the answer for how remote workers access company data.

While they have been around since the 1980's



VDI (on-premise) and now DaaS (cloud-hosted) technologies can be found in over 30% of companies around the globe.



In another 2 years, 80% of these on-prem virtual desktops will be migrated to the cloud.



At least 50% of enterprises rely on VDI for their workforce.

These are serious numbers that have tripled during the height of the pandemic. The need to retrofit an existing solution for the rapid remote employee growth has pushed desktop virtualization beyond its intent.



# In this Ebook we will explore how VDI and DaaS may be past its prime and not always the ideal solution for remote workers.

What first started in the data center, workstations have been rapidly migrating towards the public cloud.

While this has helped solve some issues, it has introduced others.

Trying to keep VDI secure can often be more challenging than anticipated.

In the last couple years, VDI/DaaS projects have been on the rise to better support remote workers but in many circumstances have hindered productivity.

The cost to deploy and support a VDI platform is often quite higher than anticipated as shown.

And finally we will look at a few alternatives to VDI and what they bring to the table.







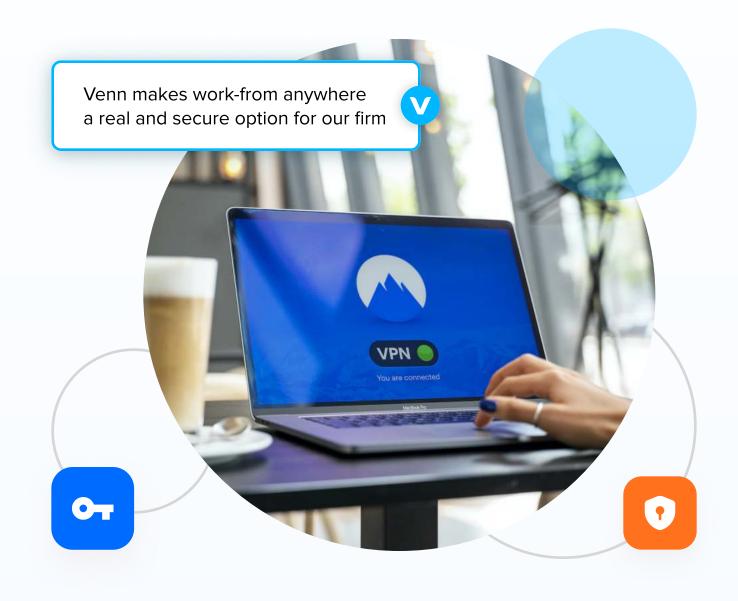
## **TABLE OF CONTENTS**

RETROFIT EXISTING TOOLS	05
THE SHIFT TO DAAS	07
KEEPING VDI SECURE	09
GETTING VDI OFF THE GROUND	12
VDI UX	14
THE HIGH COST OF VDI	16
SWITCHING TO SAAS APPS	18
SEPARATE PHYSICAL DEVICES	20
LOOKING AHEAD	22





## RETROFIT EXISTING TOOLS



In order to support these new remote-first employees, internal IT teams first looked to leverage existing legacy tools. Something that would allow workers to go home and still be productive, while keeping the company's data secure.

# The two obvious choices were VPN and VDI, each of which are tried and true technologies right?



(Virtual Private Network) creates an encrypted tunnel from your laptop back to the company's office.

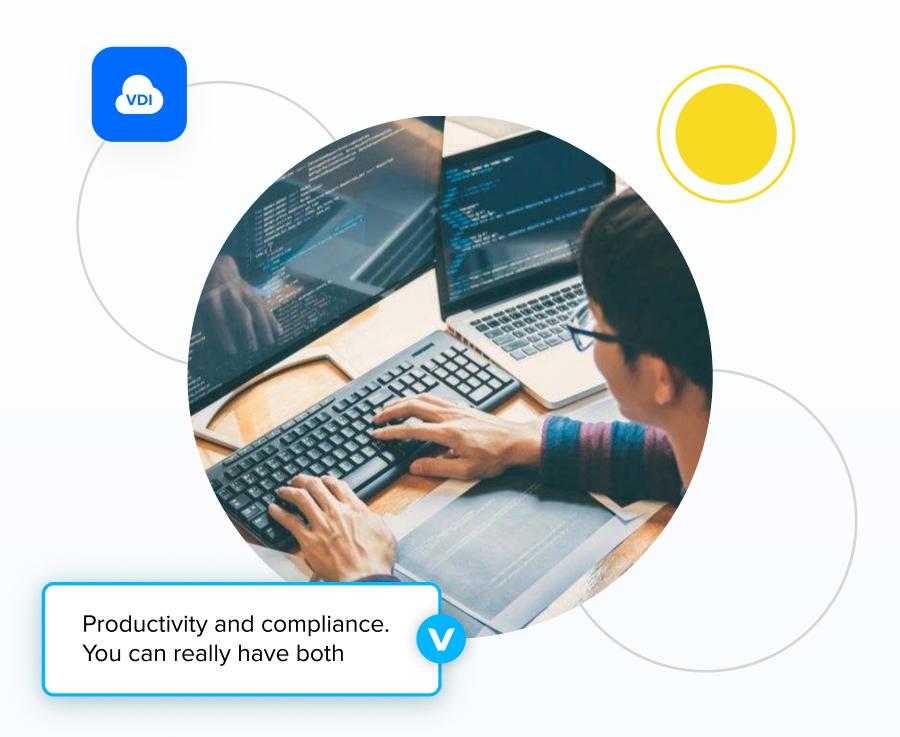


## 2 VDI

VDI, a completely different approach, allows end users to connect to a virtual desktop hosted either at the company's data center or a chosen public cloud.

While each of these help solve a subset of IT's remote-work dilemma, neither are a silver bullet and inherently introduce additional problems of their own.

#### Let's focus on VDI.





## THE SHIFT TO DAAS

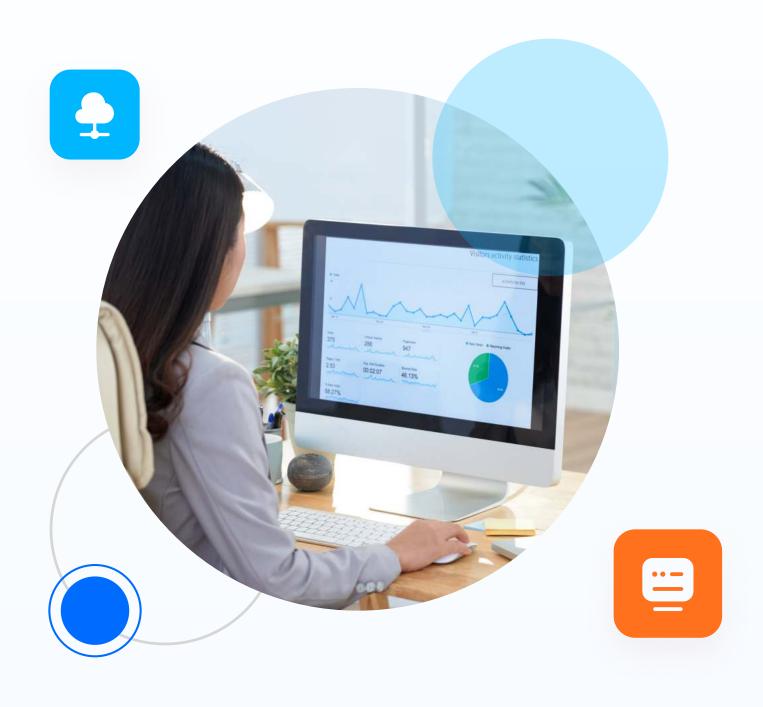
VDI attempts to keep all corporate data encapsulated in a virtual desktop that is protected by your company's various security endpoint tools, corporate Group Policies and network security controls.

By hosting these virtual desktops within the company's data center, there is more control of what gets stored inside and what is allowed to leave.

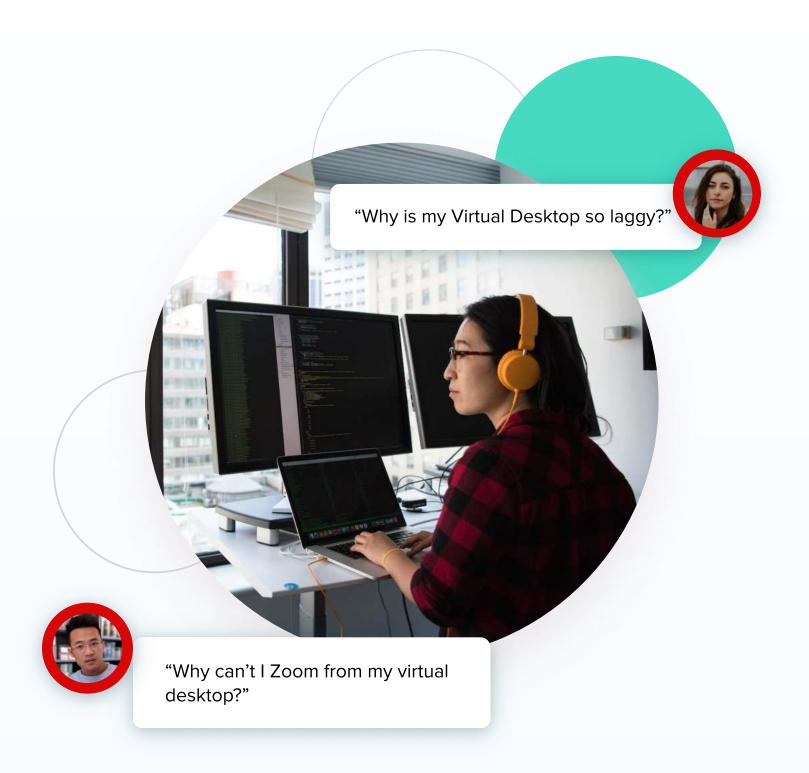
In the past few years, a shift to cloud-hosted desktops has emerged called DaaS or Desktop as a Service. This transitions the infrastructure required to host, broker and tunnel the virtual desktop connections to the cloud vendor, effectively reducing the management and operational functions for IT.

For more cloud-mature organizations this was a natural shift to move desktop workloads into the cloud, but for many starting in the height of the pandemic it became a nightmare.









## A VDI/DaaS system needs to live ideally within the same cloud and/or region to minimize latency and response time.

Once network latency, or time from a user endpoint to the virtual desktop gets over 100ms, the user experience can be degraded. You will start to experience a delay in the mouse cursor, choppy window movement or freezing while streaming and video content.

#### **FOR EXAMPLE**

If you have remote workers in Brazil accessing a virtual desktop hosted in Virginia these response times can reach over 300ms, making for an unbearable experience.

Keystrokes will be delayed, trying to talk or see a colleague on Zoom will freeze up and just using your mouse to click around through a web page will be frustrating. There are many tools like <u>this one</u> available to measure your own latency inside a given Azure region.



# This table below shows what Microsoft Azure's latency #s are from a given region to another when taken in June of 2022

Round trip Latency between Azure regions Percentile 50 (Milliseconds)	Australia Central	Australia Central 2	Australia East		Brazil South	anada	Central India	Central US	East Asia	East US	East US 2	France Central	France South	Genrmany North	Genrmany West C	Japan East	Japan West	Korea Central	Korea South	North Central US	North Europe	ıy Wes	Africa	South Africa West	Fact		Switzerland North	Switzerland West	UAE Central	UAE North	UK North	UK South	UK West	West Central Us	West Europe	West India	west oo	West US2
Australia Central	NaN		12		324 2		1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		127		212	245	235	258	250	133	140	162	155	197	259	271 2	270 3	90 40	06 18	31 9	9 13	2 24	5 241	10.00000	176	250	252	171 2	256 1	74 14	47 10	68 16:
Australia Central 2		NaN	13		325 20			185				245				134					259							3 24			177			171 2		75 14	48 1	69 16
Australia East					321 20																252 2													166				63 15
Australia SouthEast					332 2				120	215	212	236	225	248	241	118	124	145	147	200	249 2	262	261 3	82 39	98 18	86 8	8 12	3 23	5 231	167				178		66 15	54 1	75 16
Brazil South				1	NaN 13	5 145	5 300	153	319	121	118	190	199	201	195	271	277	308	310	142	175	211 2	204 3	49 3	32 14	16 33	39 31	8 20	198	297	298	184	186	167	190 2	99 1	81 1	88 16
Canada Central					Na	N 17	215	26	202	22	26	103	113	118	109	158	165	182	185	24	82 1	125	112 2	58 24	40 5	2 2	21 22	5 115	111	205	206	97	101	42	100 2	08 6	5 6	63 70
Canada East						Nat	N 224	35	211	33	36	113	124	128	119	167	174	192	197	33	95	135	122 2	68 2	50 6	2 2	31 23	8 125	5 121	215	217	107	111	51	110 2	18 7	3 7	72 82
Central India							Nat	N 233	87	201	203	125	114	136	127	124	118	115	109	221	139	147	148 2	73 28	33 23	30 5	4 3	1 12	1119	37	40	130	131	246	132	9 2	21 2	14 22
Central US																138					93 1																	41 46
East Asia											199		172	196	188	51	56		38					28 34							116	188	190	168			54 1	47 16
East US										NaN	11	86	98	101	94	159	166	184	190	24	72	107	100 2	45 2	28 3	7 22	24 21	6 98	94	192	194	79	82	43	86 1	96 6	9 6	64 57
East US 2											NaN	89	102	105	97	155	162	183	187	29	76	112	104 2	49 23	32 3	3 22	22 22	5 102	99	190	192	84	87	48	90 2	00 6	4 7	73 51
France Central												NaN	17	23	14	216	216	213	206	103	21	36	29 1	73 16	51 11	5 15	2 15	2 19	16	114	116	13	16	124	14 1	24 14	45 14	44 13
France South													NaN	30	23	206	206	203	197	113	31	44	42 1	63 17	78 12	27 14	2 14	0 17	13	103	106	23	28	136	25 1	12 1	57 1	55 14
Genrmany North														NaN	15	229	229	226	210	117	37	20	27 1	87 17	75 13	2 16			24	127	129	28	33	141	17 1	29 10	61 10	62 14
Genrmany West Central															NaN	221	221	218	212	108	28	28	26 1	78 16	57 12	3 15	7 14	2 12	16	118	121	19	25	131	21 1	21 15	56 1	51 14:
Japan East																NaN	13	35	35	145	235	241 2	240 3	861 3	76 12	8 7	3 10	8 215	5 211	153	152	221	223	123	226 1	48 1	10 10	02 11
Japan West																	NaN	42	42	152	242 2	242 2	240 3	62 3	77 13	6 8	1 10	3 216	211	147	147	221	224	130	226 1	37 1	17 1	10 118
Korea Central																		NaN	12	170	227 2	239	237 3	59 3	74 15	6 6	9 10	0 213	3 209	144	144	218	220	148	224 1	16 13	34 1	27 13
Korea South																			NaN	177	220 2	233 2	232 3	52 36	58 15	6 6	2 9	4 20	7 202	138	138	212	215	148	218 1	09 13	34 1	31 13
North Central US																				NaN	90 1	123	120 2	66 24	49 3	9 20	9 23	5 114	110	213	215	97	99	28	105 2	16 5	2 4	49 58
North Europe																					NaN	42	36 1	82 16	64 10	2 16	5 16	0 33	30	127	129	15	20	111	21 1	35 13	35 1	32 12
Norway West																					1	NaN	13 2	00 18	32 13	9 17	9 16	2 34	37	140	142	34	40	144	27 1	43 16	58 10	66 15
South Africa North																						١	NaN 1	98 17	75 13	3 17	7 16	0 31	35	139	141	28	28	146	20 1	42 17	70 1	67 15
South Africa West																							N	laN 2	2 27	75 29	97 30	4 172	168	258	261	173	173	291	183 2	71 3	14 3	311 29
South Central US																								Na	aN 26	50 31	12 31	7 172	170	274	276	155	157	273	160 2	87 2	97 2	95 28
South East Asia																									Na	N 19	5 23	0 128	3 124	217	218	110	113	28	118 2	28 3	18 4	49 24
South India																										Na	N 3	9 15	1 147	83	82	157	159	187	162	57 17	73 10	66 18
Switzerland North																											Na	N 137	7 131	50	52	157	143	219	146	24 20	05 1	98 21
Switzerland West																												Nal	N 9	113	116	25	30	135	27 1	16 15	58 1	56 14
UAE Central																																						52 14
UAE North																														NaN	10	118	121	238	124	33 20	62 2	59 23
UK North																															NaN	121	123	239	126	35 20	63 2	51 23
UK South																																NaN	12	117	13 1	27 1	41 1:	38 13
UK West																																	NaN	121	17 1	25 14	45 1	41 13
West Central Us																																		NaN '	126 2	41 3	10 2	27 38
West Europe																																		1	NaN 1	28 1	51 1	47 13
West India																																			N	aN 2	36 2	30 25
West US																																				N	aN 2	27 22
West US2																																						laN 43
West US3																																						Na

### **KEEPING VDI SECURE**

# Oftentimes the move to a virtual desktop seems to be the most secure way to provide access to corporate data.

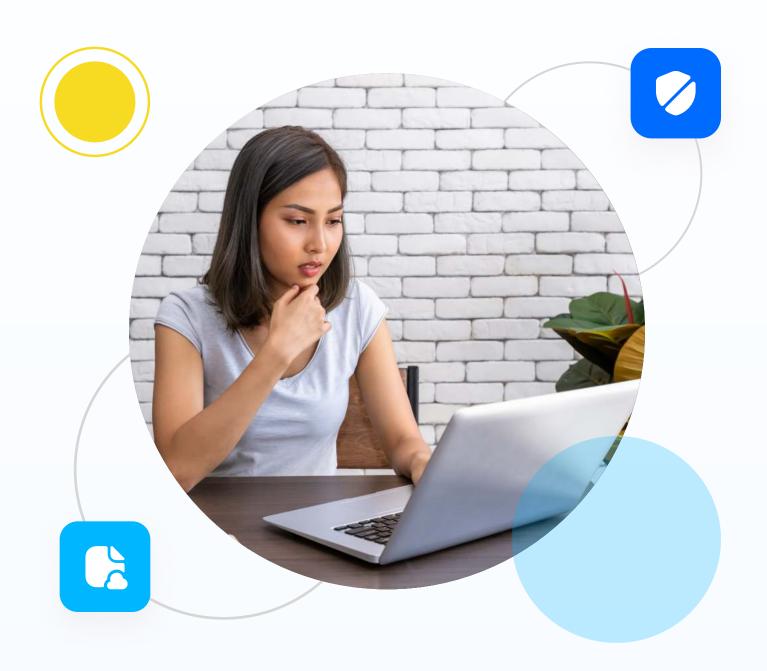
Sure, the desktop lives within the managed confines of IT and can be quickly deployed and destroyed at will. In the beginning, virtual desktops were typically accessed from a company-issued device such as a laptop.

This way the company owned the entire experience end-to-end and was able to help support any issue that may come up. Companies quickly realized that it was not very cost-effective to provide both a VDI desktop and hardware for the employee so they tried to cut costs on the physical endpoint side.

Employees were either given a low-powered Chromium device, a thinclient or asked to use their own device.







# These unmanaged devices were then left unprotected and up to the end user to keep updated.

The backend infrastructure required for VDI must remain secure and requires a neverending list of patches and updates to each of the components within.



With VDI being a known entry point for remote-workers, they are a constant attack vector for those on the interwebs looking to infiltrate and steal company data.

IT must stay up to date with the steady stream of updates needed for the infrastructure, virtual desktops and the clients used to connect.



# IT must stay up to date with the steady stream of updates needed for the infrastructure, virtual desktops and the clients used to connect.

#### **AS AN EXAMPLE**



The infamous log4j vulnerability released near the end of 2021 wreaked havoc as VDI vendors had to repeatedly apply patches upon patches each requiring their own reboots and downtime for end users.



The Windows within the virtual desktop is also another OS that must be constantly patched and rebooted as well to maintain a proper security posture.

These updates can often be scheduled after normal 9-5 hours but will still be disruptive for the end user when they login for the day and must relaunch all of their work.

With remote-workers in different time-zones this can be a challenge to accommodate and undergo the least amount of down-time.



## **GETTING VDI OFF THE GROUND**

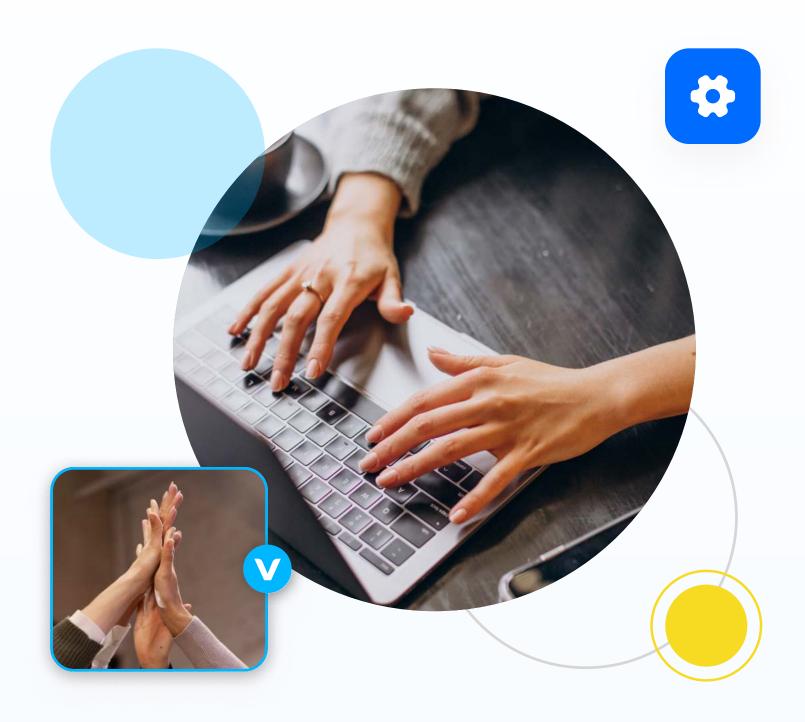
# For the 48+ million of us that did work from home during the pandemic, many had never used a virtual desktop before.

Employees were told to go home and connect to the company's VDI/DaaS environment. While introducing new technology during an already heightened period of time can be tough for end users, it can be even harder to support by untrained staff.

Often there are entire IT teams dedicated to design and manage VDI/DaaS for a company, so getting an environment spun up properly for real-world use in a matter of weeks is unfeasible.







## **Gartner**

Gartner reports that in 2020-2021, securing your remoteworkforce was the #1 project for organizations looking to review how users are accessing company apps and data.

Whether a company decides to roll out VDI themselves or hire a consultant, it can be a major effort. Several different internal teams must be involved in this effort including but not limited to:

- Desktop Support
- Server
- Networking

- Storage
- Access Control
- Firewall and more

New dedicated teams may emerge as well, responsible for the end-to-end delivery and user experience while on a virtual desktop.



## **VDI UX**

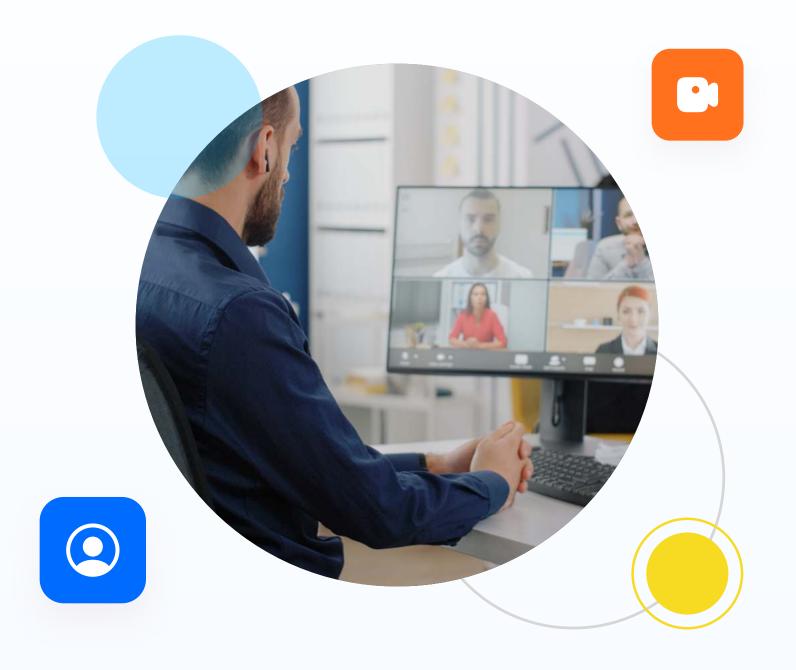
# IT often tries to suggest that virtual desktops are identical to the physical Windows desktop or laptop you've been using for years.

This enhances the comfort and trust of using a virtual desktop for the end user. That is until they try to print, copy/paste, open that large Excel file or join a Zoom video call.

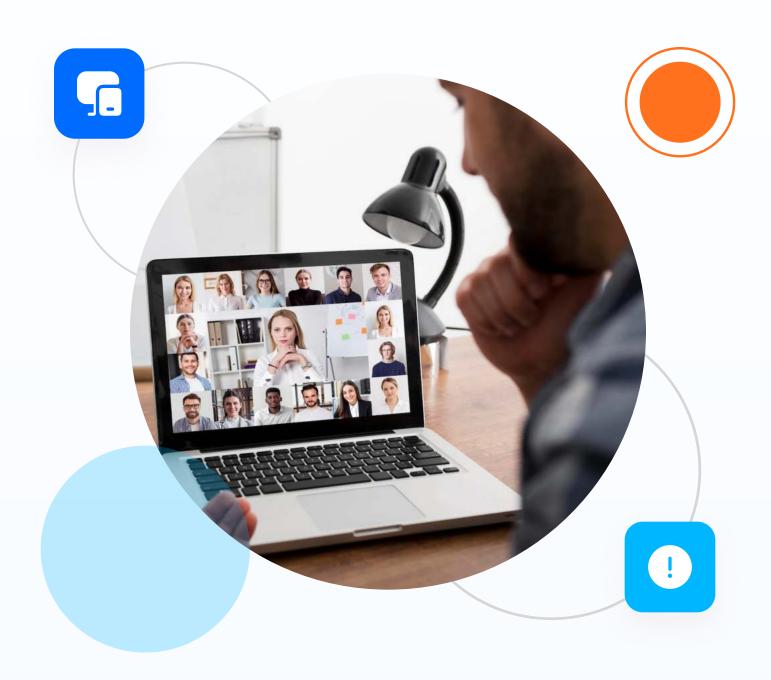
Remember, the virtual desktop lives in your public or private cloud and must traverse the various hops in between there and the printer in the office.

## verizon /

This list <u>here</u> from Verizon, shows some common apps and their bandwidth estimate per user.







As you can tell, any type of video streaming performed by a large group can often consume the organization's entire internet link if not sized properly.

And then you have a random vulnerability-scan initiated by the Security team on the network in the middle of the day.

These scans if not scoped properly can bring an entire VDI environment to its knees and consume your Help Desk staff for the day.

This reminds us that VDI lives on shared infrastructure and can suffer from the noisy neighbor problem. If 1 VM within the VDI cluster is inundated with traffic for whatever reason, it can cause others to be starving for resources. These issues and others can leave users begging for their laptop back.



### THE HIGH COST OF VDI

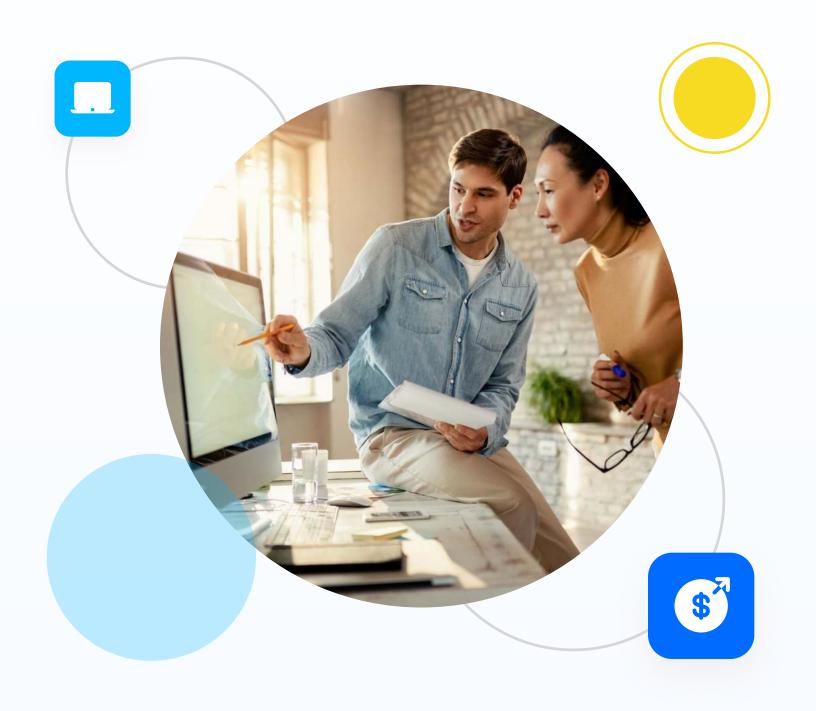
# The idea that VDI centralizes and minimizes operational costs for IT staff can also be misleading.

One of the driving forces for many companies to push employees into using a virtual desktop instead of physical machines is that they can be more efficiently managed and require less IT staff to operate.

For traditional VDI, there is still infrastructure to build, secure and manage in the data center.

The virtual desktops require IT staff to build and manage the desktop images, build and test applications and manage the access controls. In a medium to large environment, these images, applications and desktops multiply quickly and require sufficient staff to manage and support them.

While DaaS attempts to save some of the operational costs related to the hosting of the virtual desktops, the actual compute, storage and networking for the cloud-hosted virtual desktop is still a significant cost to the company, whether paid up front or monthly.





# These #s directly from Amazon, show how much an AWS Workspaces desktop can cost a single user per month:

Power	Root Volume	User Volume	Monthly Pricing	Hourly Pricing
4 vCPU, 16 GB memory	80 GB	10 GB	\$70.00	\$7.25/month + \$0.68/hour
4 vCPU, 16 GB memory	80 GB	50 GB	\$72.00	\$9.75/month + \$0.68/hour
4 vCPU, 16 GB memory	80 GB	100 GB	\$74.00	\$13.00/month + \$0.68/hour
4 vCPU, 16 GB memory	175 GB	100 GB	\$78.00	\$19.00/month + \$0.68/hour
Power Pro	Root Volume	User Volume	Monthly Pricing	Hourly Pricing
8 vCPU, 32 GB memory	Root Volume 80 GB	User Volume 10 GB	Monthly Pricing \$127.00	### ### ##############################
8 vCPU, 32 GB memory	80 GB	10 GB	\$127.00	\$7.25/month + \$1.53/hour
8 vCPU, 32 GB memory 8 vCPU, 32 GB memory	80 GB	10 GB 50 GB	\$127.00 \$130.00	\$7.25/month + \$1.53/hour \$9.75/month + \$1.53/hour

Take for example this use case of 2 different virtual profiles, Power (Marketing, Finance) & PowerPro(Developers), each using a 50 GB user volume.

[500] Power Virtual Desktops + [100] PowerPro Virtual Desktops = \$49,000 per Month

Additional headcount to manage the solution is also required. You can safely estimate another 2-3 IT Engineers (\$100k/each) needed to manage the Windows OS Images, assignments and applications tailored for DaaS. This brings DaaS costs to a minimum of \$888k per year for the organization.



## **SWITCHING TO SAAS APPS**

# So if VDI is starting to show its age and DaaS seems over-promised, overpriced and under-delivered, what might be a better fit?

One idea is to move towards a SaaS model for the more popular business systems.

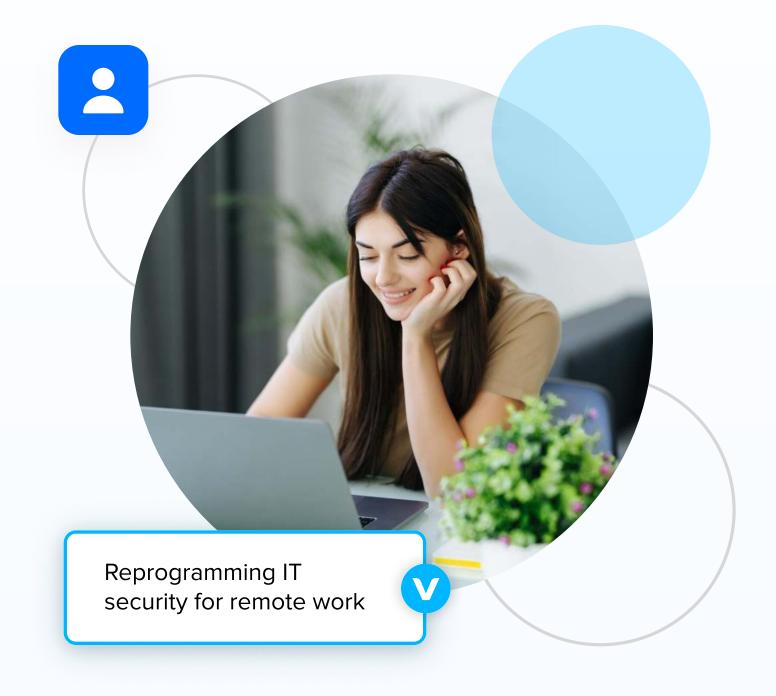
#### **APPS LIKE:**



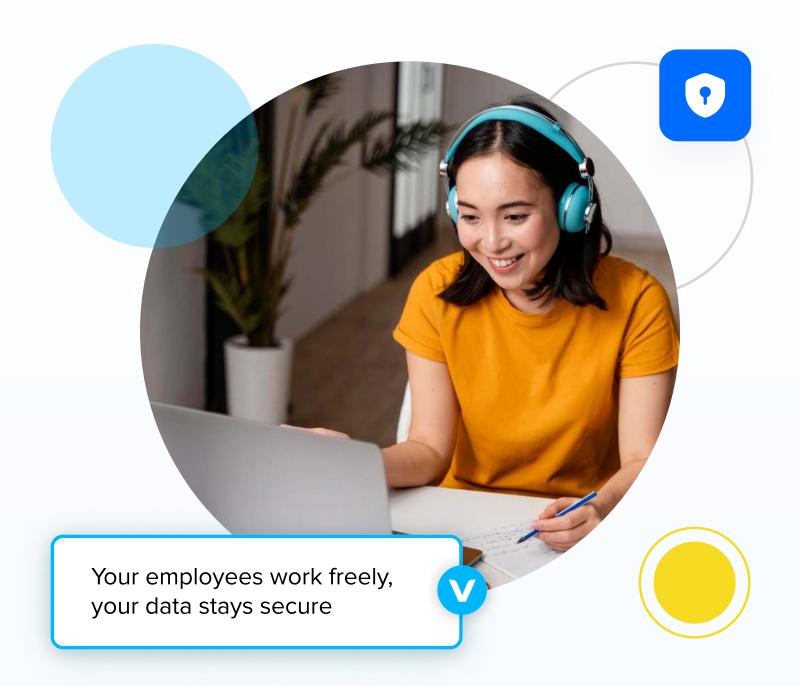
Zoom

Salesforce

These apps require no code or infrastructure to manage and can be accessed from a modern browser on any device. On average companies are using around 254 SaaS apps across the organization.









Over half of these apps are not even managed by IT, according to stats <a href="here">here</a> from Productiv.

Employees don't want to spend their time switching between browser windows lacking integration and slowing down their workflows. There can also be several security concerns when employees shift to a SaaS model such as managing sensitive corporate data in/out of web apps.

Since web apps are by nature, publicly accessible and the security controls are maintained by the vendor, some companies might have slight hesitancy on how they are used and what data is stored there.



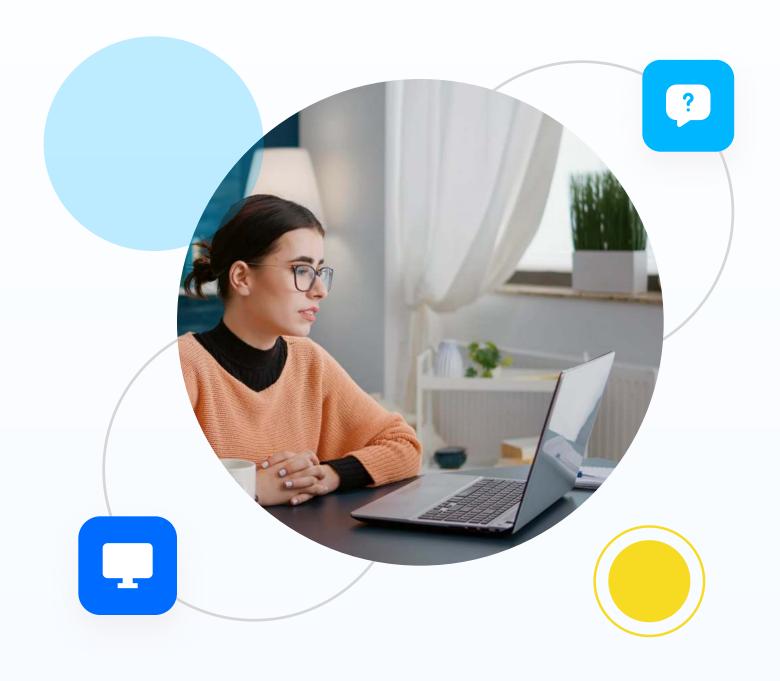
## SEPARATE PHYSICAL DEVICES

# While not a very modern approach, what about handing out laptops to any remote-first employee?

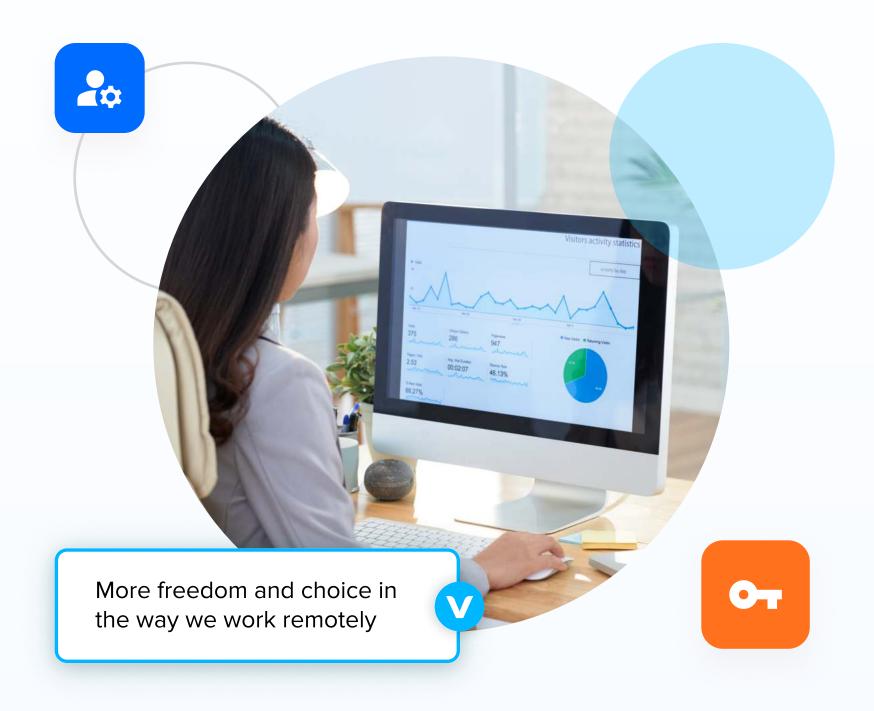
They can leverage Wifi at any location and stay connected over the company's VPN. While providing remote users a laptop is one of the most expensive options for a company to endure, it can also be insecure and unpopular as well.

With companies that have already implemented a Zero-Trust model for remote devices, the additional layers of authentication can be helpful in keeping users and devices verified but is not a complete solution.

Oftentimes a company-issued laptop will go days or even weeks without being on the VPN, missing any security patches or updates that would further harden the device.







The operational overhead to manage physical endpoints is one many companies are looking to reduce.



To learn more about the opex and capex expenses associated with managing laptops checkout this Ebook.

With companies moving towards remote-first for many of its workforce, the blend of work and personal continues to evolve.



## LOOKING FOR A MODERN VDI ALTERNATIVE

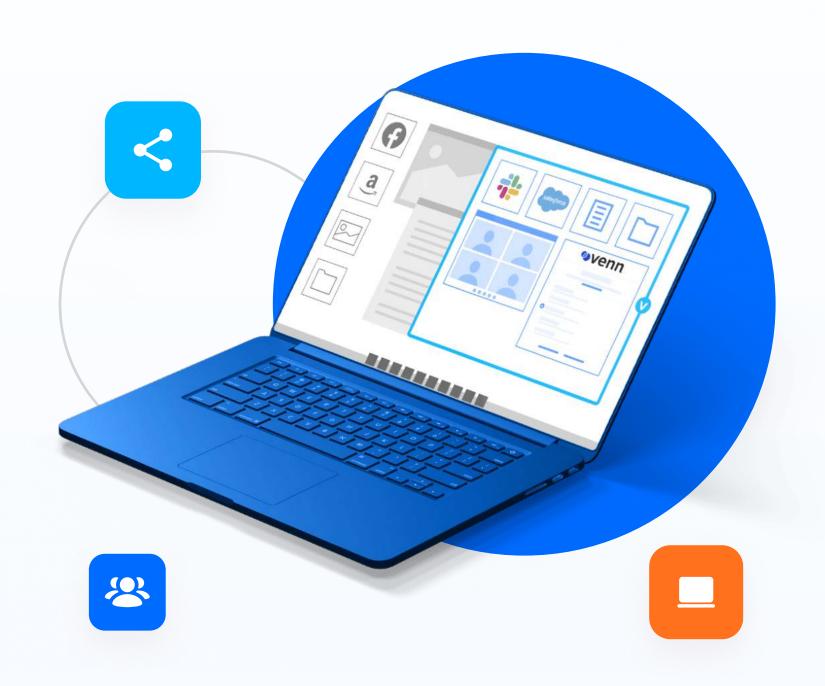
# While remote-first has become the new preferred working model for many of us, we are still waiting for a technology solution to catch up.

Employees dont want to log into multiple devices with multiple user accounts while at home. We want an experience akin to our mobile device, a single device that can handle both business and personal. One they can choose, control and balance their work and personal apps.

We don't want to manage a separate legacy device that only performs work-related tasks while they must use a different device for anything unrelated to work.

Or toggle back and forth between personal and business windows virtual desktops all day long. We need a system that allows both secure access to apps while being a platform of choice for the end user.

Until we have this euphoric solution, we must continue to balance security, cost and user experience for this new way of working.

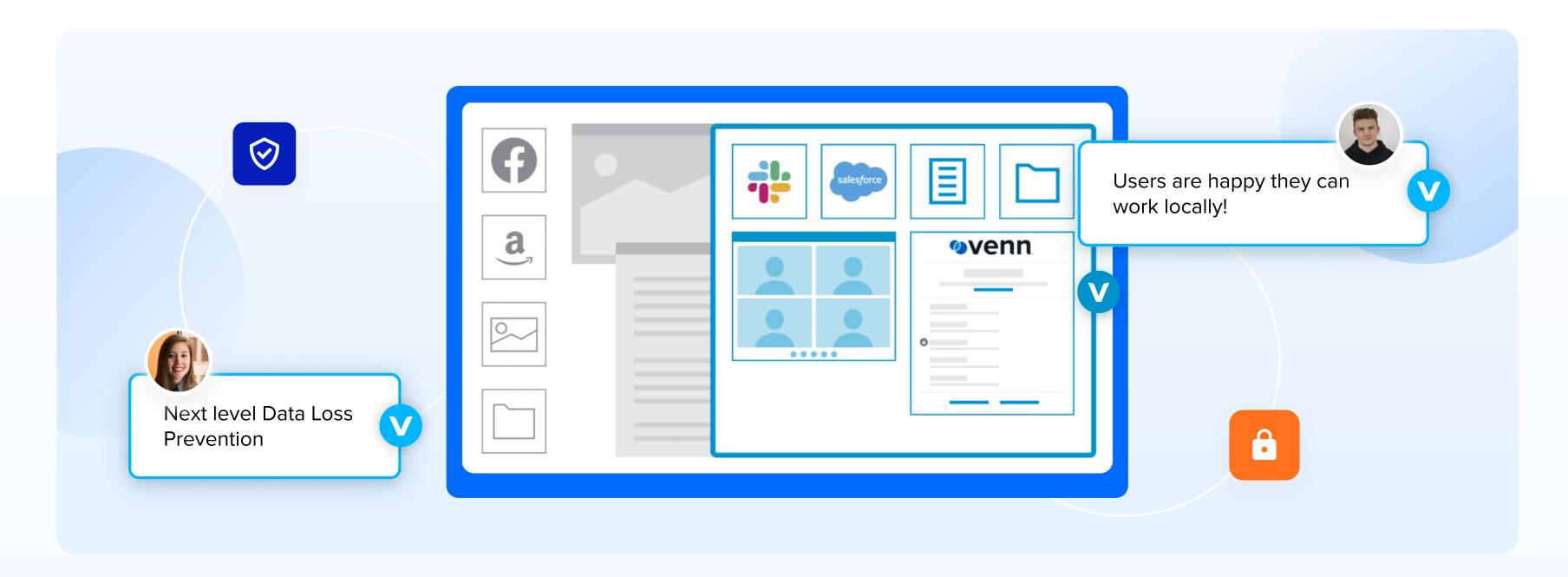




# There is a different solution, re-imagined for the modern age to overcome these preceding challenges.

A solution that is both secure and simple to manage for your existing Administrators.

Venn Software is the key to keeping company data isolated and protected in the remote-first workforce.







# Thanks for Your Attention!

Want to hear more about how Venn.com can help your company?

Book a Short Demo >

## We invite you to:

- Subscribe to get more insights and tips on this matter
- Follow us for more information about Venn's BYO-PC revolution







Linkedin