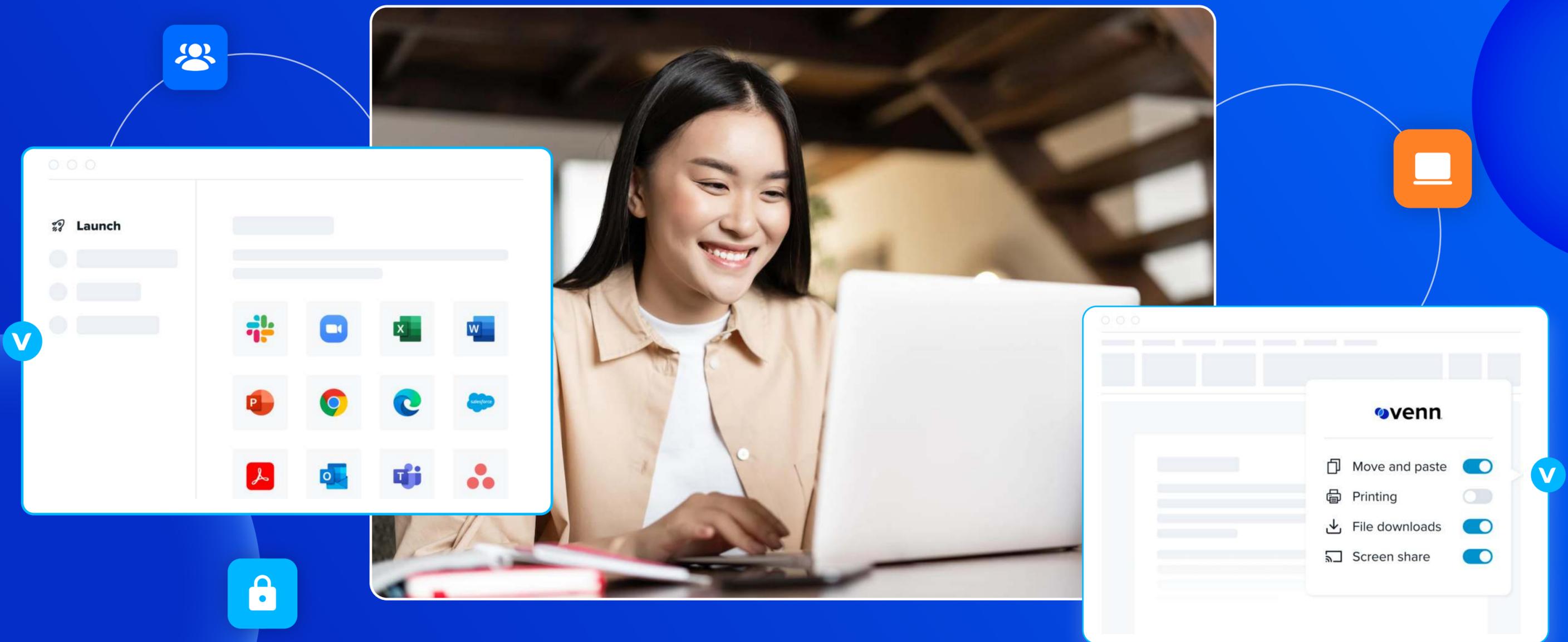


VDI Challenges for a Secure Remote Workforce



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



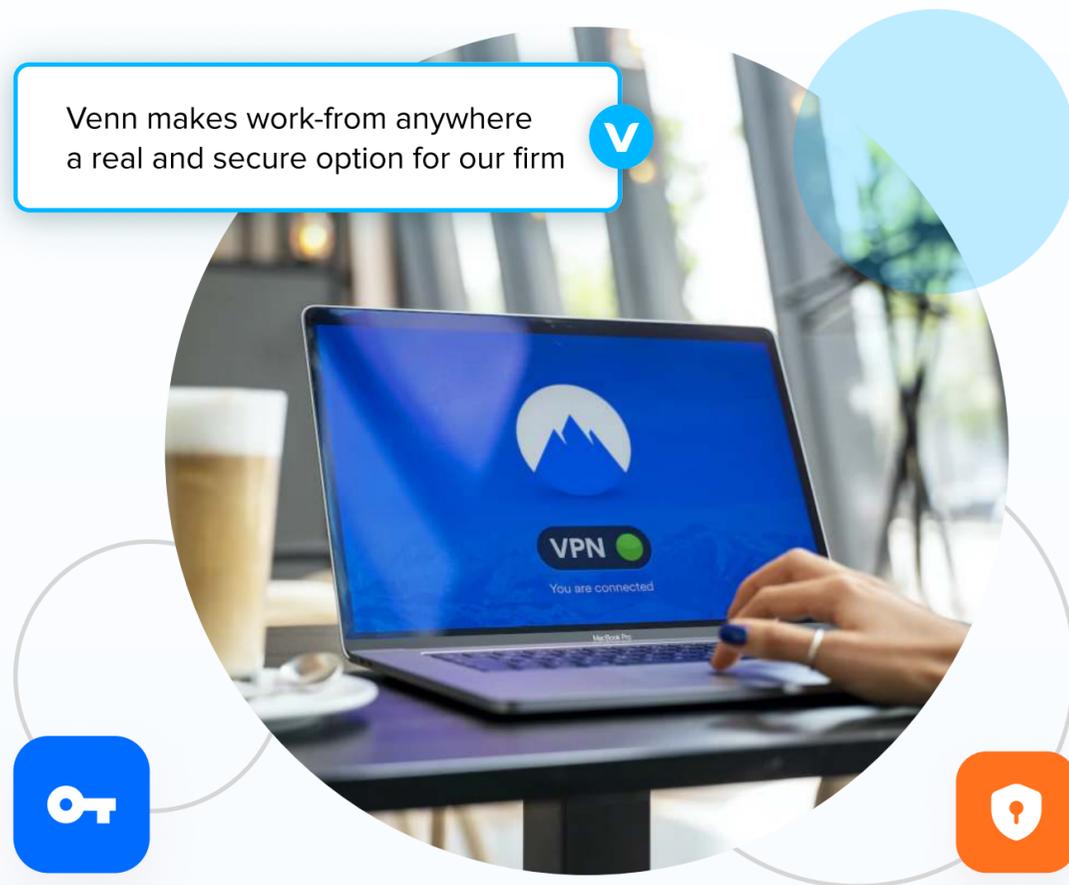
The next generation of low cost alternative to VDI



The ONLY BYO that re-frames remote work



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?

1 VPN

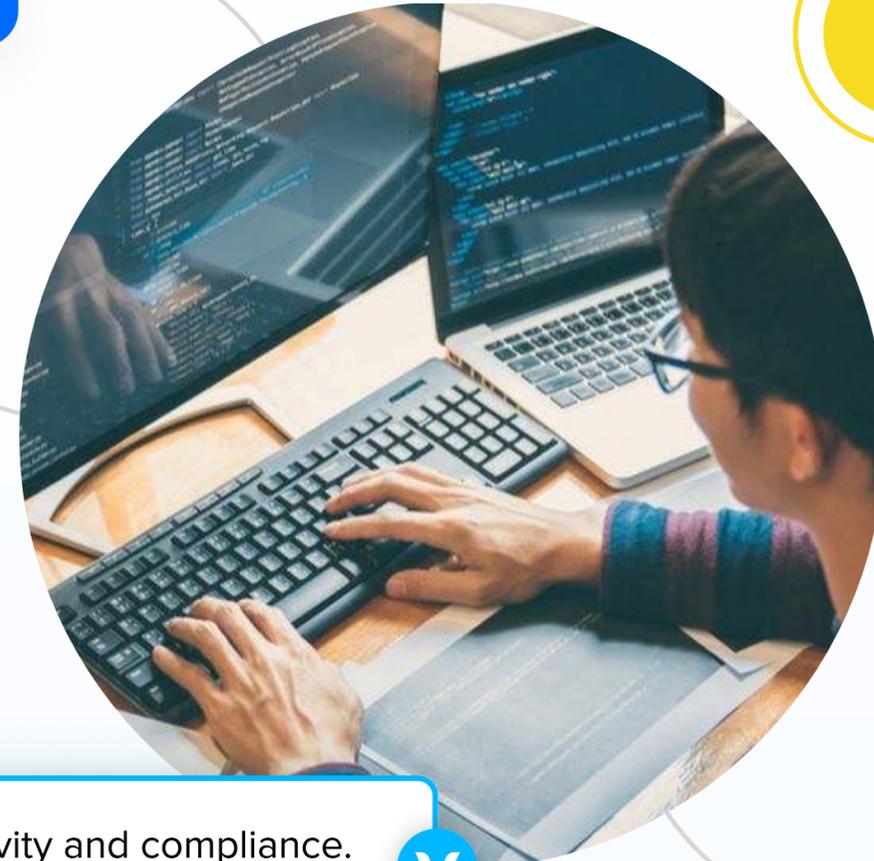
(Virtual Private Network) creates an encrypted tunnel from your laptop back to the company's office.

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.



Productivity and compliance.
You can really have both



THE SHIFT TO DAAS

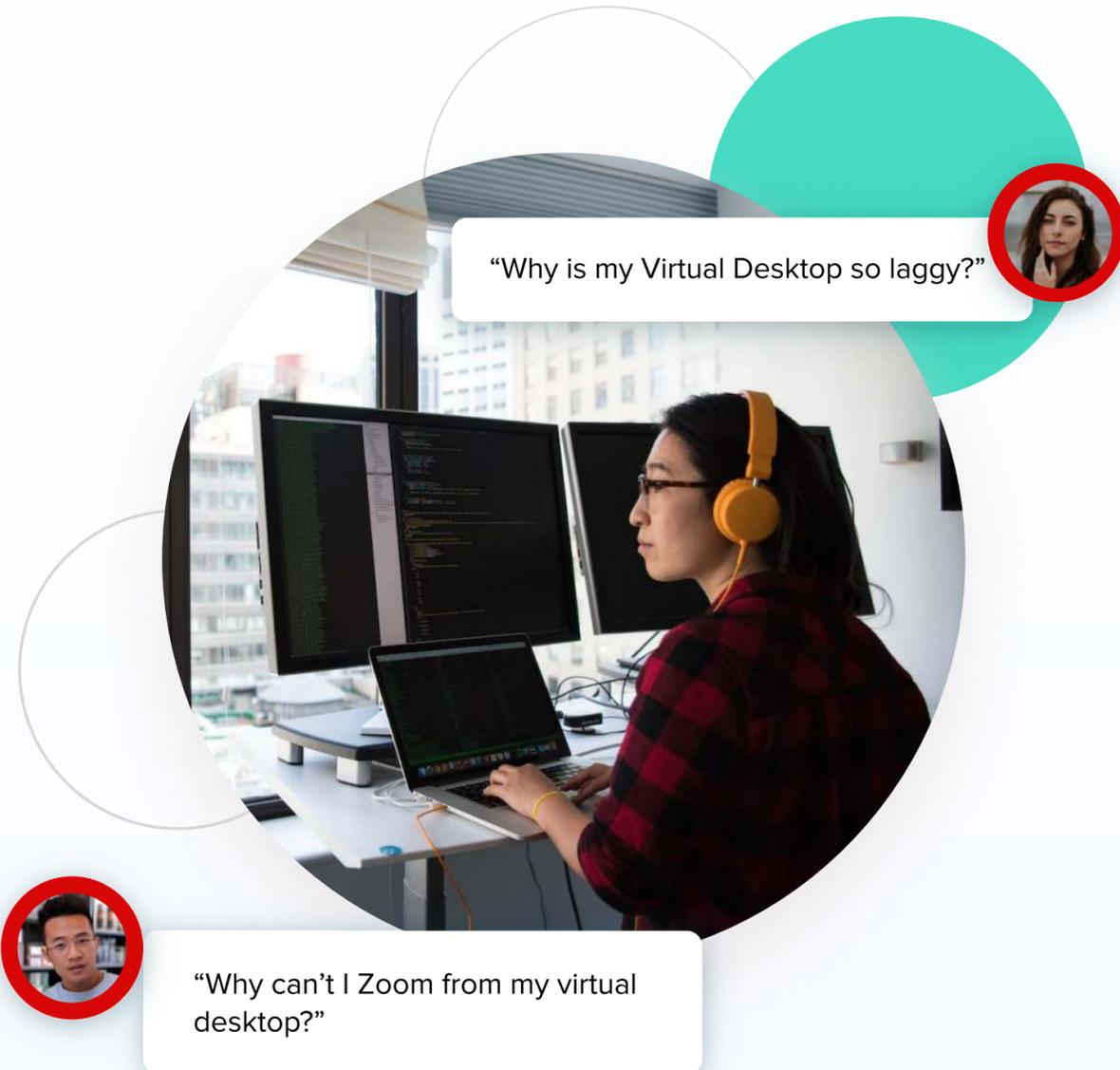
VDI attempts to keep all corporate data encapsulated in a virtual desktop that is protected by your company's various security endpoint tools, corporate Group Policies and network security controls.

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 [this one](#) available to measure your own latency inside a given Azure region.

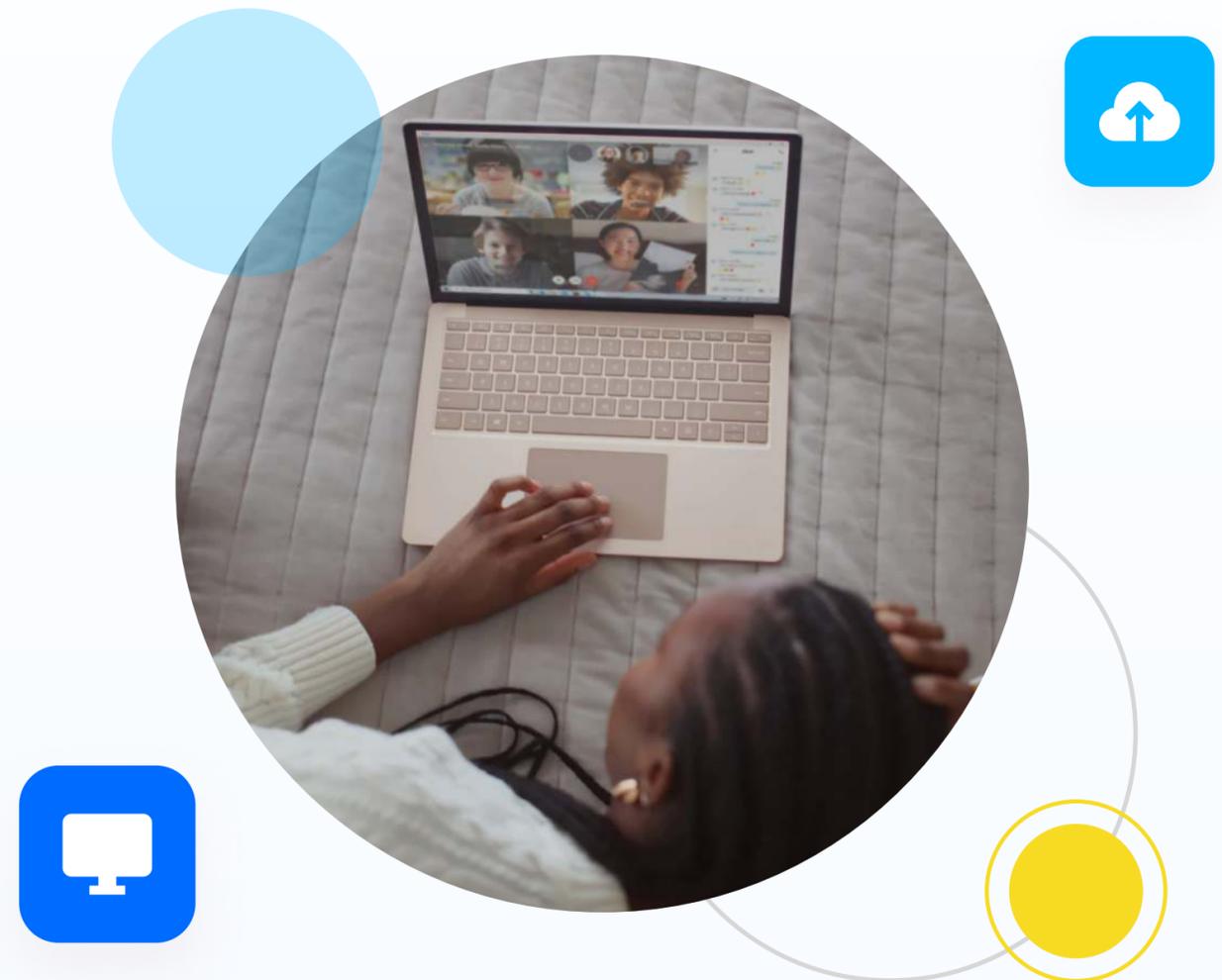
KEEPING VDI SECURE

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 thin-client 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.

V

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 remote-workforce 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^v

This list [here](#) 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

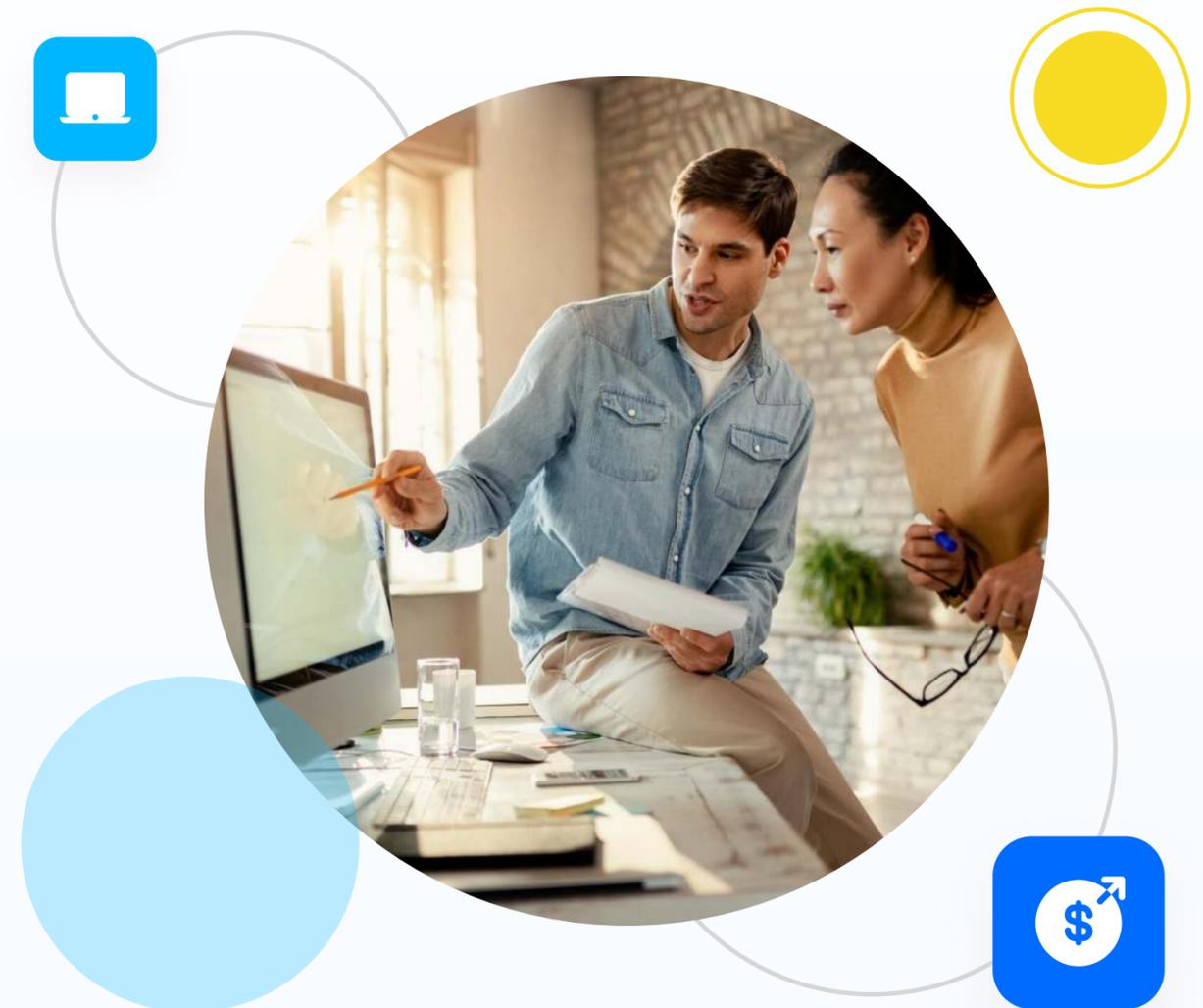
The idea that VDI centralizes and minimizes operational costs for IT staff can also be misleading.

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	80 GB	10 GB	\$127.00	\$7.25/month + \$1.53/hour
8 vCPU, 32 GB memory	80 GB	50 GB	\$130.00	\$9.75/month + \$1.53/hour
8 vCPU, 32 GB memory	80 GB	100 GB	\$134.00	\$13.00/month + \$1.53/hour
8 vCPU, 32 GB memory	175 GB	100 GB	\$140.00	\$19.00/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:

 Google Docs

 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.





Your employees work freely,
your data stays secure

 **Productiv™**

Over half of these apps are not even managed by IT,
according to stats [here](#) 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

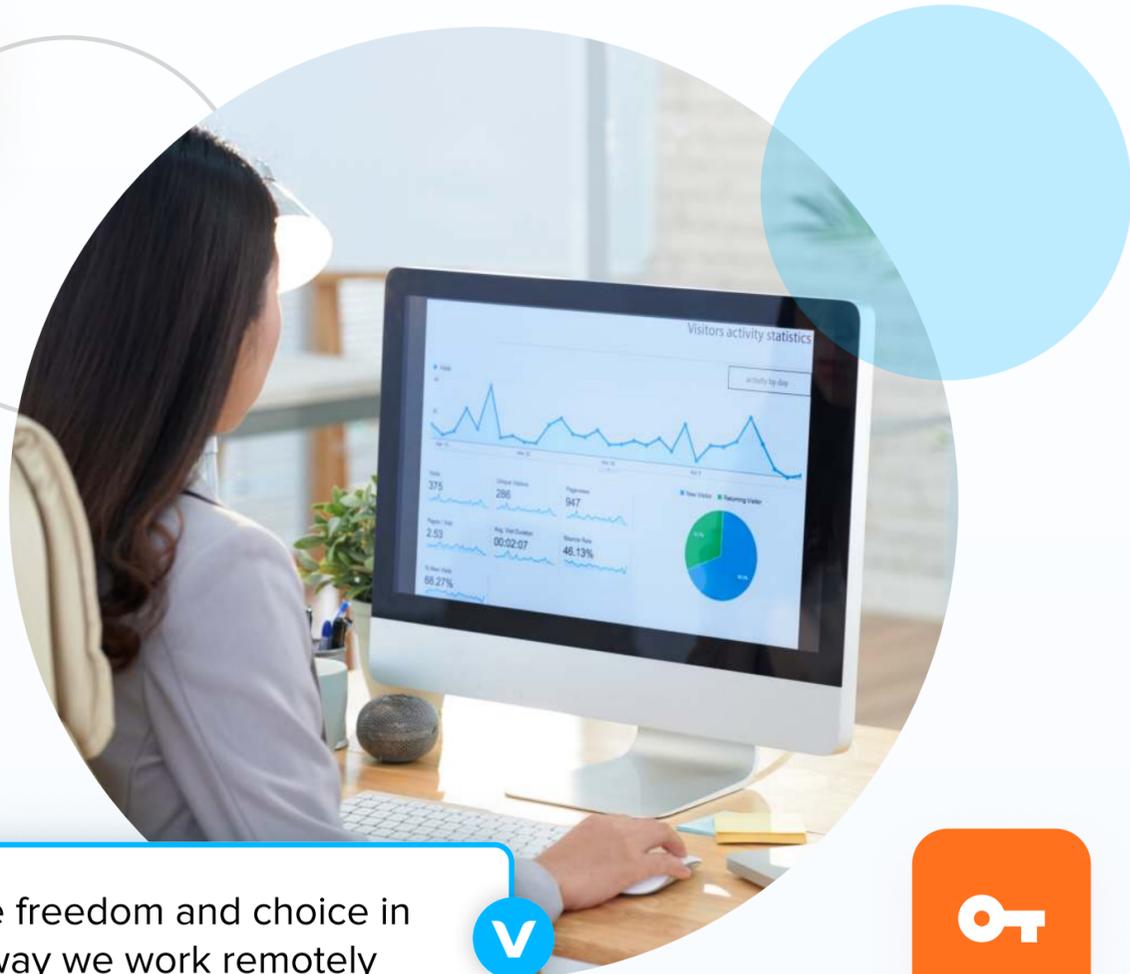
While not a very modern approach, what about handing out laptops to any remote-first employee?

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.





More freedom and choice in the way we work remotely



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 don't 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.

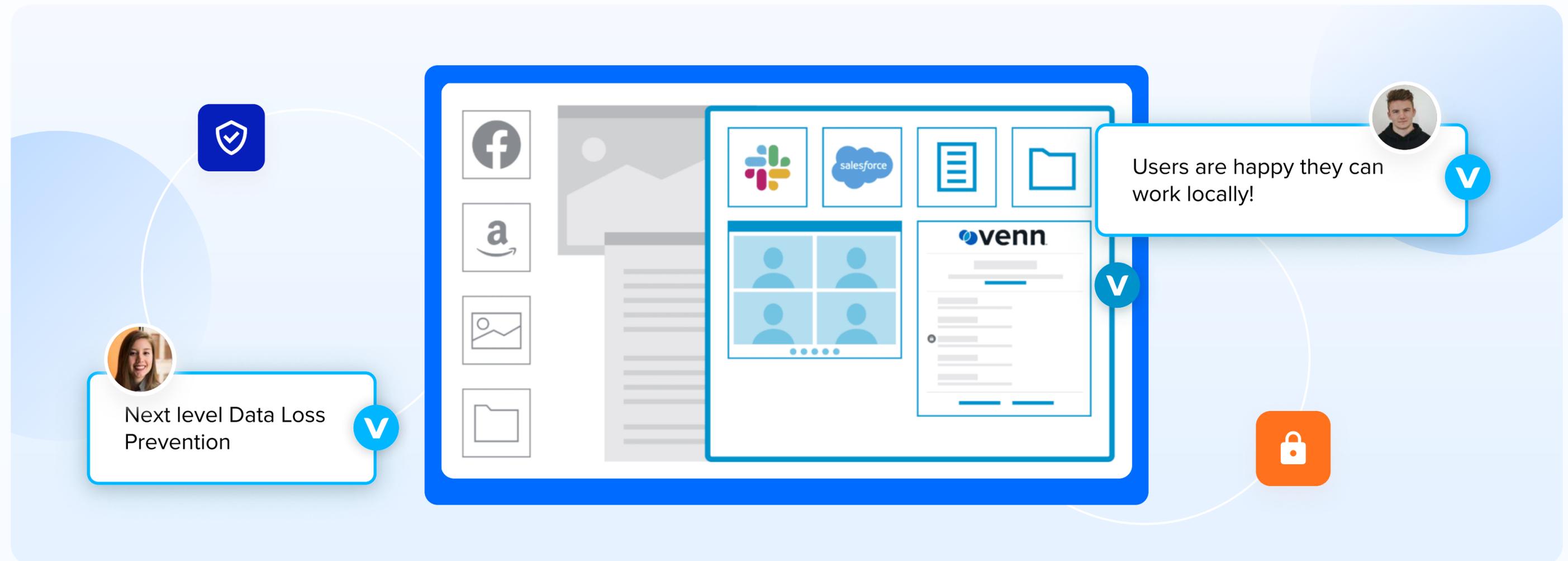
Until we have this euphoric solution, we must continue to balance security, cost and user experience for this new way of working.



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

