




# The Future Is Local


Embracing a Modern Alternative to Legacy VDI  
for Securing Remote Workers



Users are happy – that makes  
me happy!



It even works on  
my phone!



# TABLE OF CONTENTS

<b>TL;DR</b>	<b>03</b>
<b>INTRODUCTION</b>	<b>04</b>
<b>WORK IS CHANGING</b>	<b>05</b>
<b>WORKERS ARE CHANGING</b>	<b>06</b>
<b>COMPLIANCE IS TABLE STAKES</b>	<b>07</b>
<b>A EULOGY FOR VDI</b>	<b>08</b>
<b>A BRIEF HISTORY OF VIRTUAL DESKTOPS</b>	<b>09</b>
<b>5 FAILURES OF LEGACY VDI</b>	<b>10</b>
<b>LOCAL WORK DEMANDS LOCAL SOLUTIONS</b>	<b>11</b>
<b>FOUR PILLARS OF A LOCAL APPROACH</b>	<b>12</b>
<b>INTRODUCING VENN</b>	<b>15</b>
<b>VENN IS BREAKTHROUGH TECHNOLOGY, NOT A HYPERVISOR</b>	<b>18</b>
<b>SECURE REMOTE WORK ON ANY COMPUTER WITHOUT VDI</b>	<b>19</b>

# TL;DR

- Across all industries, we're undergoing a tectonic shift in where and how work gets done.
- People aren't balancing work and life. They're integrating them into a continuous, modern mode of existence. They expect their devices and IT policies to keep up.
- Hybrid work on more devices combined with rising employee expectations around experience and privacy have created a new mandate for IT and security teams.
- Virtual Desktop Infrastructure (VDI) comes up short in addressing this mandate, forcing users to find workarounds to get their jobs done.
- The new reality of modern work has eroded the promise and potential of VDI, IT teams and security pros with the Herculean task of repurposing VDI solutions to solve challenges the infrastructure wasn't designed for.
- The only way to truly ensure productivity, protection and privacy in the modern mode of work is to empower users to work locally, not hosted.
- Venn® is a new secure workspace designed to deliver the security and compliance benefits of legacy Virtual Desktop Infrastructure (VDI) with a simpler and more cost-effective solution that users love.
- With Venn, the future is local.



The only way to truly ensure productivity, protection and privacy in the modern mode of work is to empower users to work locally, not hosted.



# INTRODUCTION

**Today in 2023 we are seeing that remote and hybrid work are here to stay and models like BYOD, SaaS and mobile devices are pervasive to the point of being commonplace.**

But despite beliefs that the pandemic changed everything (which it did in many ways), so many of these now de facto IT approaches were already well underway long before COVID hit. The virus simply accelerated many of the changes that were in play, most notably the move to videoconferencing as the default way of meeting.

As for VDI, despite much innovation and progress, virtual desktop penetration is still only a small fraction of overall end-user computing — well under 10%.

**The reality is that the industry has been struggling with the failed promise of VDI for some time. We're still waiting on that proverbial "Year of VDI."**

Unfortunately, there continues to be forces too formidable for virtual desktops to overcome: trying to keep up with the performance and experience expectations of modern devices; the multimedia and real-time communication requirements of videoconferencing; compatibility issues with a diverse desktop and mobile OS application ecosystem; and so much more.

As we look at the virtual desktop landscape across industries, this report offers a reflection on where we've been, with major implications for where we're going. It presents a view toward the future. More IT and security leaders, as well as MSPs, are realizing that "The Future is Local". They're looking beyond the shortcomings of legacy VDI solutions to new alternatives that harness the power of local platforms and processing power.

They recognize that the only way to truly secure work in today's world is to see protection and productivity not as opposing forces, but as common goals that empower users to do and be their best. They're reimagining what's possible in a post-VDI world.





# WORK IS CHANGING

*Across all industries, we're undergoing a tectonic shift in where and how work gets done, along with employee expectations around how organizations should support that work. We're working from more places on more devices than ever before.*

*People aren't balancing work and life. They're integrating them into a continuous, modern mode of existence. Devices keep us connected, and flexibility empowers us to balance professional and personal tasks on our own schedule.*

*It's a new reality with massive implications for IT and security professionals – especially in security and compliance-driven organizations. For these organizations, effective cybersecurity has become a business imperative. The IT-risk scape is fast evolving, and legacy security solutions are struggling to keep up.*

A recent report from DTEX reveals that due to the rise of insider threats as a result of the work from anywhere trend, there has been a **72%** growth in actionable insider threat incidents, with theft of either data or intellectual property being the most common leaks.<sup>1</sup>

## 5 GREATEST CYBERSECURITY THREATS FACING ORGANIZATIONS TODAY



### Ransomware

Ransomware will cost its victims around \$265 billion (USD) annually by 2031. The dollar figure is based on 30 percent year-over-year growth in damage costs over the next 10 years.<sup>3</sup>



### Third-party software

Within Web Application attacks, 80% involved stolen credentials.<sup>4</sup>



### Accidental or Malicious Exfiltration

There has been a 72% year-over-year growth in actionable insider threat incidents, with theft of either data or intellectual property being the most common leaks.



### Social engineering (phishing, scareware)

Successful spear phishing attacks account for 95% of breaches in enterprise networks.<sup>5</sup>



### Cloud Computing Vulnerabilities

65-70% of all security issues in the cloud start with a misconfiguration.<sup>6</sup>

According to IBM, **more than 50%** of new work-from-home employees are using their own personal computers for business use, however 61% also say their employer hasn't provided tools to properly secure those devices.<sup>2</sup>

## SOURCES

1. [www.cybernews.com/security/remote-work-and-the-rise-of-insider-threats/](https://www.cybernews.com/security/remote-work-and-the-rise-of-insider-threats/)
2. [www.newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk](https://www.newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk)
3. [www.cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/](https://www.cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/)
4. [www.verizon.com/business/resources/Tbaa/reports/dbir/2022-data-breach-investigations-report-dbir.pdf](https://www.verizon.com/business/resources/Tbaa/reports/dbir/2022-data-breach-investigations-report-dbir.pdf)
5. [www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats](https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats)
6. [www.trendmicro.com/en\\_us/research/21/a/the-top-worry-in-cloud-security-for-2021.htm](https://www.trendmicro.com/en_us/research/21/a/the-top-worry-in-cloud-security-for-2021.htm)

# WORKERS ARE CHANGING

As knowledge workers embrace the kitchen table, home office and coffee shop workspaces and connect with colleagues and clients on their personal phones, tablets and laptops, their technology expectations are higher than ever. They expect a seamless experience no matter how they're working or what device they're on. They expect organizations to support that experience, and they have no issues bypassing or ignoring IT security policies and protocols to get that experience.

At the same time, today's employees expect a greater degree of personal privacy, even as "life" creeps further into the work/life equation.

## Gartner

**"Less than 50% of employees trust their organization with their data, and 44% don't receive any information regarding the data collected about them.<sup>7</sup>**

In 2021, new regulations will emerge at the state and local level that will start to put limits on what employers can track about their employees."

## The Harris Poll

According to a recent Venn/Harris Poll study, **nearly three-quarters (71%) of employed Americans (full or part time)**, have done something to get around their company's IT policy or procedures in order to be more productive and efficient at their job.<sup>8</sup>

### SOURCES

7. [www.gartner.com/smarterwithgartner/9-work-trends-that-hr-leaders-cant-ignore-in-2021/](https://www.gartner.com/smarterwithgartner/9-work-trends-that-hr-leaders-cant-ignore-in-2021/)

8. This survey was conducted online within the United States by The Harris Poll on behalf of Venn between August 10-12, 2022 among 994 adults who are employed full time or part time. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated. For complete survey methodology, including weighting variables and subgroup sample sizes, please contact [marketing@venn.com](mailto:marketing@venn.com).

# COMPLIANCE IS TABLE STAKES

Even as cybersecurity regulations and reporting requirements grow more onerous, leading organizations today are developing cybersecurity objectives beyond mere compliance with FINRA, HIPAA, SEC, NAIC, and SOC 2 standards. Hybrid work on more devices combined with rising employee expectations around experience and privacy have created a new mandate for IT and security teams to hold themselves to a higher standard

## ORGANIZATIONS TODAY ARE LOOKING FOR SOLUTIONS THAT SATISFY THREE AREAS.



### End User Productivity

Empowering users to work locally the way they want on the device of their choice from anywhere.



### Security & Compliance

Ensuring regulatory compliance and protecting work files and data from accidental or malicious exfiltration, compromise or loss.



### Rapid Onboarding

Onboard and offboard remote workers in minutes.

These three goals share an intricate interplay, where favoring one too heavily threatens the integrity of the other two.

Organizations find themselves navigating a complex balance with an outdated and outmoded set of tools and approaches.



# A EULOGY FOR VDI

## VIRTUAL DESKTOPS WERE SUPPOSED TO BE THE ANSWER.

For the last two decades, virtual desktop infrastructure (VDI) approaches have been the go-to data security and compliance solution for security and compliance-driven organizations. By removing business applications and data from user endpoints and hosting them in the cloud, IT teams gained a level of visibility and control. VDI served as a centralized security and compliance solution with rudimentary levels of data loss prevention.


## THE TRADITIONAL VDI MODEL WORKED – FOR A WHILE.

There was a time not so very long ago when most knowledge workers worked from a single Windows desktop to access mostly Windows applications. Many in regulated industries worked from a virtualized desktop with a fixed endpoint device that never left their offices. Others had laptops they would bring between work and home or use personal Windows machines to send emails in the evening or work over the weekend.


It was a simpler time, and virtual desktops were well suited to it. The virtual workspaces abstracted business software and sensitive data from the local host operating environment, providing better remote protection and security.

## THE WORLD IS A LOT MORE COMPLICATED TODAY.

Nearly every IT trend of the last decade has served to undercut VDI as an economic and empowering solution for IT teams and end users. SaaS offerings. Mobile devices. BYOD. Apple's resurgence in personal computing. Work from home. Hybrid workplaces. Each exciting new reality of modern work has eroded the promise and potential of VDI, leaving IT teams and security pros with the Herculean task of repurposing VDI tools to solve for challenges the infrastructure wasn't designed for.



I can't tell whether I'm in my virtual desktop or not!



Why can't I Zoom from my virtual desktop?

VDI

SaaS

# A BRIEF HISTORY OF VIRTUAL DESKTOPS

When virtual desktops first burst onto the scene, Michael Jordan was making his triumphant return to the NBA. DVDs were invented, and Toy Story (the first one) premiered. It was a revolutionary time for the tech industry, with the rise of the consumer internet and the first real steps toward the technologies that would allow computing for business and personal uses to happen from anywhere. Here's a closer look at how Virtual Desktops got started and how we got to where we are today.



**1995**

*Citrix WinFrame launches*



**1998**

*Microsoft releases Windows NT 4.0 Terminal Server Edition*



**2004**

*VMWare introduces Virtual Desktop Infrastructure (VDI)*



**2014**

*Amazon Web Services (AWS) launches Workspaces, the first hyperscale cloud Desktop as a Service (DaaS) offering*



**2021**

*Microsoft introduces Windows 365Cloud PC*



## WHAT'S NEXT

*Venn introduces the industry's first [Virtual Desktop alternative for securing remote work on any BYOD laptop](#)*



## VIRTUAL DESKTOP INFRASTRUCTURE (VDI):

is a desktop virtualization technology wherein a desktop operating system, typically Microsoft Windows, runs and is managed in a data center.

## DESKTOP AS A SERVICE (DAAS):

is a cloud computing offering in which a third party hosts the back end of a virtual desktop infrastructure (VDI) deployment



# 5 FAILURES OF LEGACY VDI



## 1. Unacceptable Performance

Virtual desktops are at an inherent performance disadvantage compared to working locally. With a user in one location and desktop, applications and data in another, the experience is highly dependent on network latency. Slow application launch times, lags and sluggish performance are the inevitable result. As end user devices get faster and flashier, lethargic VDI approaches fall even further out of step with modern demands.



## 2. Unfamiliar Experience

The way we interact with technology is hardwired into our brains. We perform our most familiar tasks via muscle memory, and we expect order and consistency when it comes to navigating our desktop and essential applications. Virtual desktops disrupt that experience and flow, sending user frustrations soaring and productivity plunging. And for most Mac users, what could be more foreign and unwanted than being forced to remotely connect to a virtualized Windows environment to do their work?



## 3. Unusable Video Meetings

Videoconferencing adoption and acceptance leapt forward at least a decade as a result of COVID-19. Many teams rely on Zoom, Skype, WebEx by Cisco, Microsoft Teams and more to communicate with colleagues and clients. Yet the videoconference experience via a virtual desktop is abysmal – if it works at all. The overwhelming majority of users bypass their virtual desktops and security protocols and run conferencing solutions locally on their devices – often based on guidance from their IT teams.



## 4. Unsited for SaaS

Browser-based applications have transformed the market for business software over the past decade, with the majority of critical platforms (e.g., CRM, ERP, etc.) having migrated from traditional client-server architectures to SaaS models. That evolution greatly reduces the benefits of virtual desktops, effectively limiting them to platforms for running a remote web browser – providing an abysmal experience in the process. Users are quick to bypass virtual desktops and access SaaS applications directly, creating visibility gaps and significant compliance and security threats.



## 5. Untenable Mobile Access

The growth of mobile applications has mimicked SaaS adoption and further exposed the weaknesses of virtual desktops. While vendors continue to tout the ability to access hosted applications and desktops from mobile devices, the truth is that very few, if any, users leverage this functionality after their first attempt. Anyone who's ever tried to pinch and zoom via remote access on a phone knows why. There are significant performance and usability challenges that hinder work and foster unsecure access.

**Employees are having eight extra meetings a week and communicate even more with their colleagues since remote work became the new normal, a recent study finds.<sup>9</sup>**

### SOURCES

9. The University of Texas - Austin Researchers - [studyfinds.org/remote-workers-more-meetings/](https://studyfinds.org/remote-workers-more-meetings/)



# LOCAL WORK DEMANDS LOCAL SOLUTIONS



The only way to truly ensure productivity, protection and privacy in the modern mode of work is to empower those users to work locally. That means accessing applications, SaaS platforms, files and data natively without relying on traditional on-premise VDI or cloud-hosted Desktop-as-a-Service resources.

A genuine local solution leverages the power and flexibility of modern devices (desktops, laptops, tablets, and smartphones) and their local browser-, desktop- or mobile-based applications, regardless of the application's deployment method (user-installed or IT managed). It eliminates the compatibility and performance issues associated with legacy VDI solutions.

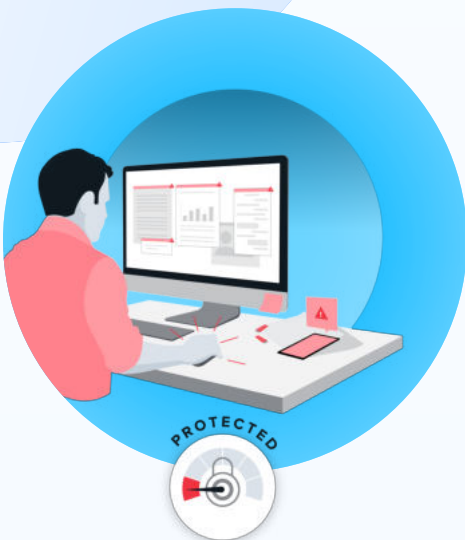
**Traditionally, local solutions delivered that superior experience, but left critical gaps in data security and compliance via unrestricted access.**

That's clearly not an option for most organizations today – especially with ever-expanding compliance considerations. The future is local – with some important considerations.

## ACCELERATION OF REMOTE WORK

There's no shortage of commentary and analysis around COVID-19's impact on the working world. The pandemic has driven a surge in virtual and hybrid workspace adoption, leaving IT and security pros to come up with meaningful solutions with limited time and budgets.

But the reality is, while COVID-19 may have accelerated and accentuated technologies like video conferencing and remote work, it certainly didn't create them. Future-focused organizations have seen these trends coming for some time, and many recognized VDI's lackluster performance in this new reality.



*Unrestricted local access  
is no longer an option*

# FOUR PILLARS OF A LOCAL APPROACH

## 1. USER-CENTRIC – DELIVER AN ENHANCED EXPERIENCE

Employees expect technology to work with little need for calibration or compromise. As more and more organizations adopt remote and hybrid work models, delivering that enhanced user experience will become essential to recruiting and retaining top talent.

### The Security/Workaround Paradox

Today's regulated and security and compliance-driven businesses face a complex and costly paradox.

The more security protocols they put in place to curb cyberthreats and curtail risky user behavior, the more employees' digital experience suffers, and the more users find workarounds to get their jobs done. Each new workaround undermines compliance and exposes the organization to costly security threats.

And it's only getting worse. Users are accessing more data on more devices all the time. New productivity and communication tools like videoconferencing apps create new compatibility challenges. Employees are managing more personal activities – checking personal email, placing orders on Amazon, alongside their professional work, and they expect a layer of privacy in those activities.

As a result, it's users and those workarounds that ultimately decide compliance, leaving IT and security teams to chase down new shortcuts and react to threats and exposures rather than proactively foster a secure environment.

A local solution creates opportunities to unravel this costly paradox, but only if the solution delivers the experience users expect.

Apple's resurgence in personal computing. Work from home. Hybrid workplaces. Each exciting new reality of modern work has eroded the promise and potential of VDI, leaving IT teams and security pros with the Herculean task of repurposing VDI tools to solve challenges the infrastructure wasn't designed for.



**48%** of employees want to be fully remote and **44%** want a hybrid work model.<sup>10</sup>

### SOURCES

10. [www.salary.com/news-and-events/83-percent-of-employees-would-leave-job-if-compensated-less-for-remote-work/](https://www.salary.com/news-and-events/83-percent-of-employees-would-leave-job-if-compensated-less-for-remote-work/)

## 2. RISK-CENTRIC – SOLVE FOR THE NEW AND NUANCED RISKS OF MODERN WORK

COVID may not have created the remote and hybrid workspace trend, but it sure has accelerated it. That modern mode of work has created a new set of security risks and compliance challenges for IT teams to see and solve.

### 3 Emerging Dangers of the New Risk-scape

- Increased Ransomware and Cyber Threats – Bad actors recognize the opportunity for malicious acts lurking in users working from home.
- BYOD Security – Policies be damned. People are using their own devices to access sensitive company data.
- Distracted or Untrained Users – Employees may be rethinking their work/life balance, but that overlap creates opportunities for distractions as social engineering attacks that rely on human error increase.

## 3. LIFE-CENTRIC – PROVIDE SEAMLESS WORK/LIFE TOGGLING

As employees navigate remote and hybrid models and do more and more work from personal or shared devices, everyday life is creeping into the employee experience. Solutions are needed that allow users to keep professional and personal activities separate and distinct – without compromising the tech experience. Increasingly, that's becoming an HR imperative with a direct impact on employee satisfaction and retention rates.

### Employers will shift from managing the employee experience to managing the life experience of their employees.<sup>14</sup>

Gartner's 2020 Reimagine HR Employee Survey found that employers that support employees with their life experience see a tangible increase (more than 20%) in the number of employees reporting better mental and physical health. Supportive employers can also realize a 21% increase in the number of high performers compared to organizations that don't provide that same degree of support to their employees. In 2021, employer support for the entire employee life experience will become table stakes in employee benefits."

**238%**

There has been a **238% increase** in global cyberattack volume during the pandemic.<sup>11</sup>

**TWO-THIRDS**

**Two-thirds** of people use their own devices at work, regardless of the company's BYOD policy.<sup>12</sup>

**85%**

**85%** of breaches in 2020 involved a human element.<sup>13</sup>

### SOURCES

11. [threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/](https://threatresearch.ext.hp.com/hp-wolf-security-blurred-lines-blindspots-report-risky-remote-working/)
12. [www.microsoft.com/security/blog/2012/07/26/byod-is-it-good-bad-or-ugly-from-the-user-viewpoint/](https://www.microsoft.com/security/blog/2012/07/26/byod-is-it-good-bad-or-ugly-from-the-user-viewpoint/)
13. [www.verizon.com/business/resources/reports/dbir/](https://www.verizon.com/business/resources/reports/dbir/)
14. [www.gartner.com/smarterwithgartner/what-is-the-new-employment-deal/](https://www.gartner.com/smarterwithgartner/what-is-the-new-employment-deal/)

## 4. FUTURE-CENTRIC – REALIZING A DISTRIBUTED, SCALABLE ALTERNATIVE

Remote work trends underscored by the pandemic and the evolving workplace aren't going away any time soon. Local or not, organizations need solutions that satisfy current and future business goals. One thing is clear: The risks of failing to develop a modern and future-centric solution are simply too great to ignore.

### The Hidden Costs of Failed IT Security Solutions



#### Computing Costs

- CapEx and OpEx Investments
- Maintenance and Upgrades
- Training and Enforcement



#### Culture Costs

- Declining User Satisfaction
- Policy Updates and Training
- Turnover and Retention Challenges



#### Client Costs

- Communication Gaps
- Delays and Frustrations
- Turnover and Slowed Growth



#### Compliance Costs

- Fines
- Audit Requirements
- Bad Press and Distractions



# INTRODUCING VENN

**Venn has invented a new approach to securing remote work on any unmanaged computer without VDI.**

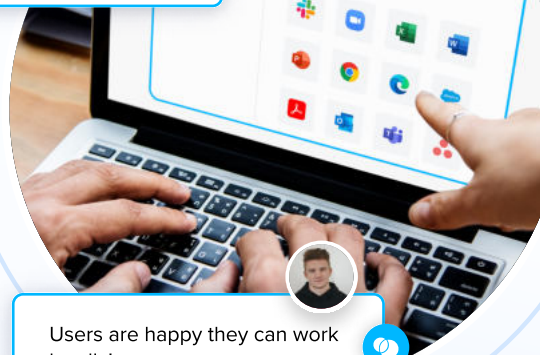
**Venn** is the first purpose-built patented technology for Secure BYO-PC. Venn secures remote work on any unmanaged or BYOD computer with a radically simplified and less costly solution than virtual desktops or having to lock down every PC. Similar to an MDM solution but for laptops – work lives in a company-controlled secure enclave installed on the user's PC or Mac, where all data is encrypted and access is managed. Work applications run locally within the enclave – visually indicated by the Blue Border™ – where business activity is isolated and protected from any personal use on the same computer.

Company data is now protected without having to control the entire device, and as a result, remote work is secured without the cost, complexity and performance issues of VDI. As happened in the past with mobile phones, employees want to use their preferred computer – not have one for work and one for personal – while companies are eager for ways to avoid buying, shipping and locking down computers.

**With Venn, work applications run locally within a secure enclave – visually indicated by the Blue Border™ – that isolates and protects business activity from any personal use on the same computer.**



Next level Data Loss Prevention.



Users are happy they can work locally!





**Venn is driving the future of Secure BYO-PC without VDI. By inventing a new patented approach to securing remote work on any computer, Venn provides companies with a radically simplified and less costly solution than virtual desktops or having to lock down every PC.**

## **VIRTUAL DESKTOP ALTERNATIVE**

Virtual Desktop Infrastructure, which has long been the de facto approach to protecting apps and data on remote and unmanaged computers, is increasingly being recognized as a less-than-ideal choice. VDI is complex, expensive and often frustrates users. It's redundant for browser-based applications and doesn't perform well with video applications. A new approach is needed.

Venn is the leading virtual desktop alternative for securing remote work. Security and compliance-driven organizations can now easily protect company data on any unmanaged or BYOD computer without the cost and complexity of VDI.

**Venn unlocks a new level of productivity by allowing users to work locally with none of the lag or compatibility challenges introduced by VDI.**

Venn enables companies to achieve a level of compliance, control, and visibility needed into today's hybrid work environment and increasingly risky cybersecurity landscape. With Venn, organizations can achieve all this without the sluggish performance and cumbersome user experience of legacy VDI.

It also enables them to seamlessly toggle back and forth between their work and personal digital lives on the same device without exposing their organization to data loss and leakage or subjecting their personal computing resources to monitoring by their employer.



## THE BLUE BORDER™

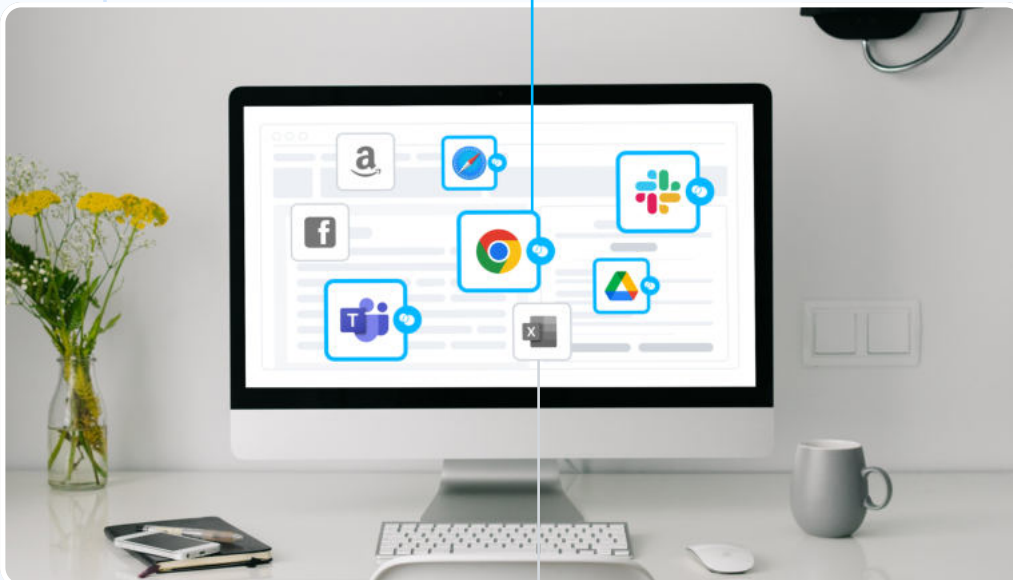
What happens in the Blue Border stays in the Blue Border.

Inside the secure enclave, business activity is isolated and protected from any personal use on the same computer. Data loss prevention is successfully accomplished by keeping work data inside the enclave and by keeping potential threats and malicious software out. This is similar to today's MDM solutions but for laptops now, not just for phones.

The Blue Border provides full administrative control over work applications and data running inside the secure enclave. Similar to an MDM solution, but for laptops – remote work can now easily be secured on any PC or Mac without VDI. Security and compliance-driven organizations can now easily protect company data on any managed, unmanaged or BYOD computer without the cost and complexity of virtual desktops.



Work application are wrapped by a **Blue Border**



Personal applications walled off from work

# VENN

## IS BREAKTHROUGH TECHNOLOGY, NOT A HYPERVISOR

Venn provides a new approach to app, file and data isolation, which breaks the accepted paradigm that in order to protect sensitive work applications and data, they must somehow be abstracted or virtualized away from the user's host OS (e.g., VDI, client hypervisor, etc.). Unlike a client hypervisor such as Parallels Desktop, Venn does not virtualize the entire operating system.

Through sophisticated application, filesystem and network isolation techniques, Venn enables desktop, browser-based and mobile work applications, files and data to safely and securely co-exist alongside a user's personal digital assets on a desktop, laptop or mobile device. This enables applications to run as intended, with responsive performance and none of the compatibility issues normally associated with VDI.

Venn is also the first solution that clearly distinguishes work resources from personal apps and information so that users know exactly what is protected, managed and monitored by their organization and what is not.

**Venn is the leading virtual desktop alternative  
for enabling Secure BYO-PC.**



# SECURE REMOTE WORK ON ANY COMPUTER WITHOUT VDI



## Security & Compliance

Protects company data from accidental or malicious compromise or loss.



## Cost

Reduces or eliminates the cost and complexity of buying, managing and securing company-owned PCs and/or Virtual Desktop Infrastructure.



## User Convenience & Privacy

Enables users to have a single computer with clear separation between work and private personal uses.



## Control

Enables robust administrative controls over work applications and data including policies for network access, peripheral use, copy-paste and more.



## Easy Deployment

Integrates with existing infrastructure. Onboard and Offboard users in minutes.



## WELCOME TO THE FUTURE

The modern mode of work demands a modern approach to balance user productivity and privacy. It has to be user-centric, risk-centric, life-centric, and future-centric. Given these demands and ever evolving challenges, legacy VDI approaches simply won't cut it.

**With Venn, the Future is Local for Securing Remote Workers.**





# Are you ready to make the shift from legacy VDI to Venn?

Book a demo with our experts and experience Venn's breakthrough technology. We are excited to help you and your team stay productive and, protected, and work the way you most prefer.

Venn is the leading solution for securing remote work without VDI. Security and compliance-driven organizations can now easily protect company data on any BYOD or unmanaged computer without the cost and complexity of virtual desktops. Over 700 organizations, including Fidelity, Guardian, and Voya, trust Venn to meet FINRA, SEC, NAIC, and SOC 2 standards.

[Book a Short Demo](#) >



Venn deploys in minutes.



Apps work with no lag – even Zoom!



[Website](#)



[Blog](#)



[LinkedIn](#)