venn

The Future Is Local

EMBRACING A MODERN ALTERNATIVE TO LEGACY VDI

Table of Contents

venn

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, leaving MSPs, IT teams and security pros with the Herculean task of repurposing VDI solutions to solve for 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.
- The Venn® Zero Trust Platform (ZTP) is the industry's first Virtual Desktop Alternative (VDA) that delivers the centralized management and critical information security benefits of legacy Virtual Desktop Infrastructure (VDI) along with additional essential cybersecurity capabilities that are not a part of standard VDI offerings.
- 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.

venn

Foreword

I was first introduced to the concept of virtual desktops back in the summer of ’95. I was about a year into my first job in the IT world and immediately saw the potential for keeping people secure in remote settings.

That summer began my obsession in solving enterprise IT challenges, leading me to long-productive partnerships with a number of innovators as I collected my share of related certifications (starting with Citrix WinFrame 1.7). Now, 25 years later, the tech has changed and the risks have exploded, but the core goals remain the same: ensure the highest levels of protection, privacy and productivity in a fast-changing world.

As I write this, I’m sitting in a Starbucks on the Upper East Side of Manhattan, typing away on a laptop while swiping through work emails on my personal phone. I realize that I have been working remotely in some capacity for most of my career. However, back then I was the exception.

Now, remote work is the rule 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.

So here we are in the summer of ’21. Despite remarkable 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.

JEFF FISHER | VP OF STRATEGY

Jeff Fisher has more than 20 years of experience developing and implementing go-to-market strategies for several notable emerging and growth-stage infrastructure software companies. He is currently Vice President of Strategy at Venn where he leads a number of GTM elements of the company's Zero Trust Platform and LocalZone™ technology. Jeff previously served as Vice President of Strategy and/or Alliances for Softricity (acquired by Microsoft), Desktone (acquired by VMware), RES Software (acquired by Ivanti) and KEMP Technologies. Jeff has also held technical sales and business development roles at Microsoft and Citrix. He earned a B.A. degree from Cornell University and an M.B.A. from Columbia Business School.

venn

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 MSPs, IT and security professionals – especially in regulated and security-minded organizations. For these firms, effective cybersecurity has become a business imperative. The IT-risk scape is fast evolving, and legacy security solutions are struggling to keep up.

Forrester predicts that due to pandemic-related uncertainty, remote work conditions, and employee experience, **one-third (33%)** of security breaches will be caused by insider threats in the coming year.[1]

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.[2]

5 Greatest Cybersecurity Threats Facing Organizations Today

RANSOMWARE

Ransomware damage costs are predicted to grow more than 57X from 2015 to 2021, and reach $20 billion[3]

THIRD-PARTY SOFTWARE

Web applications account for more than 80% of all documented data breaches[4]

SOCIAL ENGINEERING (phishing, scareware)

Successful spear phishing attacks account for 95% of breaches in enterprise networks[5]

DDOS ATTACKS

DDoS attacks increased +19% in Q2 2021 compared to Q1 2021[6]

CLOUD COMPUTING VULNERABILITIES

65-70% of all security issues in the cloud start with a misconfiguration[7]

SOURCE

[1] https://www.code42.com/resources/reports/forrester-paper-predictions-2021-cybersecurity
[2] https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to- Working-from-Home-Pose-Security-Risk
[3] https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2019-to-2021/
[4] https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf
[5] https://www.securitymagazine.com/articles/94506-5-biggest-cybersecurity-threats
[6] https://www.helpnetsecurity.com/2021/07/21/ddos-attacks-h1-2021/
[7] 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 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.

"LESS THAN 50% OF EMPLOYEES TRUST THEIR ORGANIZATION WITH THEIR DATA, AND 44% DON'T RECEIVE ANY INFORMATION REGARDING THE DATA COLLECTED ABOUT THEM.[8]
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."

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.[9]

SOURCE

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

[9] This survey was conducted online within the United States by The Harris Poll on behalf of Venn between August 10-12, 2021 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.

venn

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, 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.

PRODUCTIVITY

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

PROTECTION

Protecting work files and data from accidental or malicious exfiltration, compromise or loss

PRIVACY

Separating digital work from personal computing and ensuring non-work activities are not monitored

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 regulated and security-minded firms. 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.

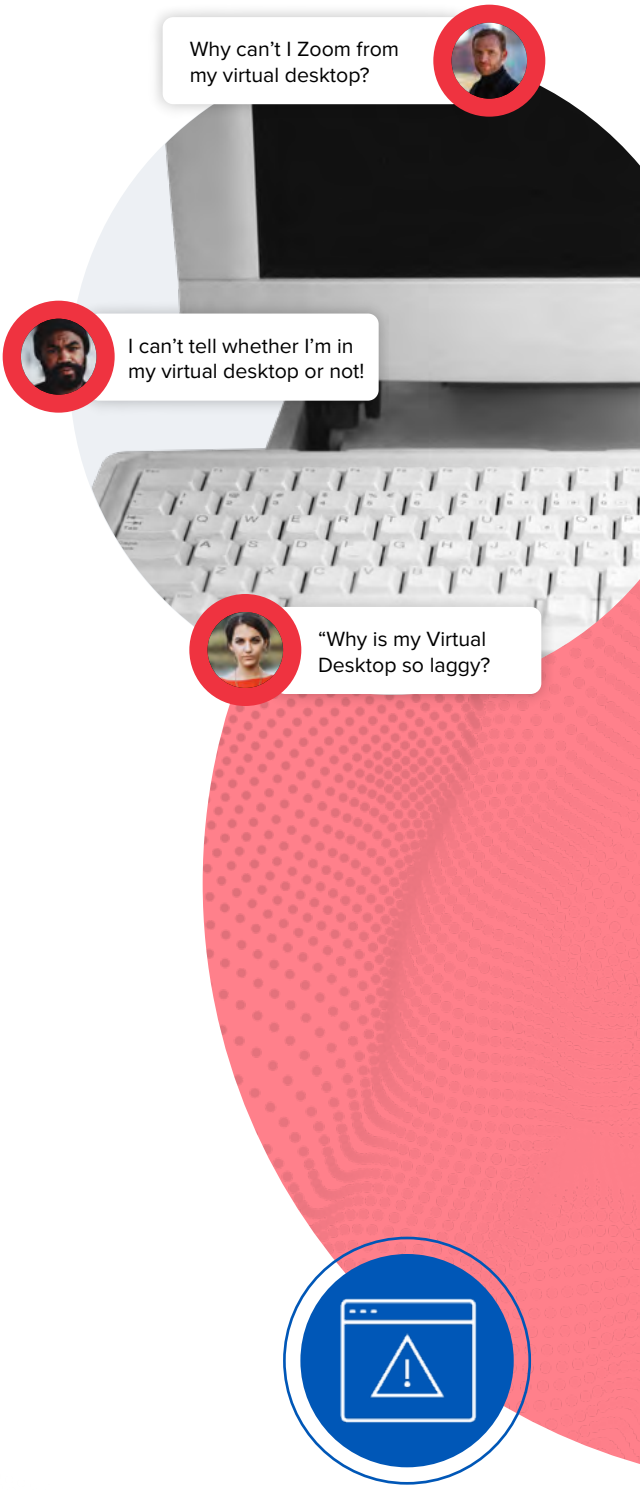
THE TRADITIONAL VDI MODEL WORKED – FOR A WHILE.

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 MSPs, IT teams and security pros with the Herculean task of repurposing VDI tools to solve for challenges the infrastructure wasn't designed for.



venn

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, powered by LocalZone™

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.

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. UNSUITED 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.

84% of remote workers conduct at least one meeting via video conference per week.[10]

SOURCE

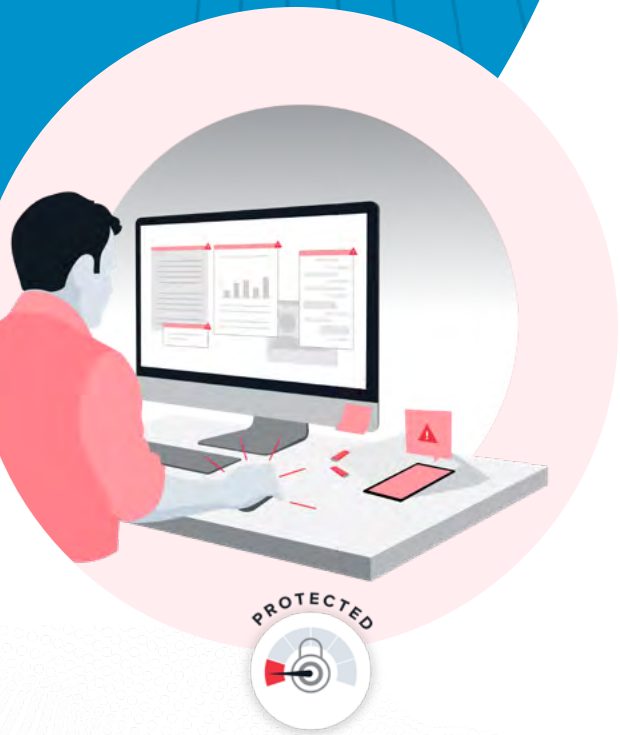
[10] https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-Employees-New-to-Working-from-Home-Pose-Security-Risk

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.*



Unrestricted local access is no longer an option

That's clearly not an option for most firms 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 MSPs, 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.

venn

4 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-minded businesses face a complex and costly paradox.

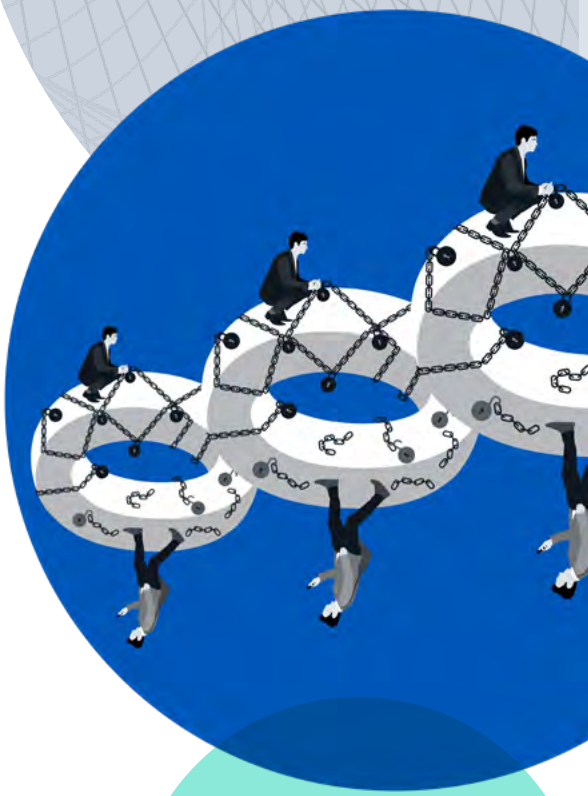
The more security protocols they put in place to curb cyberthreats and curtail risky user behavior, the more employees' digital experience suffers, and the more users find workarounds to get their jobs done. Each new workaround undermines compliance and exposes the organization to costly security threats.

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 MSPs, IT teams and security pros with the Herculean task of repurposing VDI tools to solve for challenges the infrastructure wasn't designed for.



48% of employees want to be fully remote and **44%** want a hybrid work model.[11]

SOURCE

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

There has been a **238% increase** in global cyberattack volume during the pandemic.[12]

Two-thirds of people use their own devices at work, regardless of the company's BYOD policy[13]

85% of breaches in 2020 involved a human element.[14]

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

1. **Increased Ransomware and Cyber Threats –** Bad actors recognize the opportunity for malicious acts lurking in users working from home.
2. **BYOD Security –** Policies be damned. People are using their own devices to access sensitive company data.
3. **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. Local solutions 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.[15]

Gartner's 2020 ReimagineHR 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."

SOURCE

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

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

The trends underscored by COVID-19 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 Ops 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

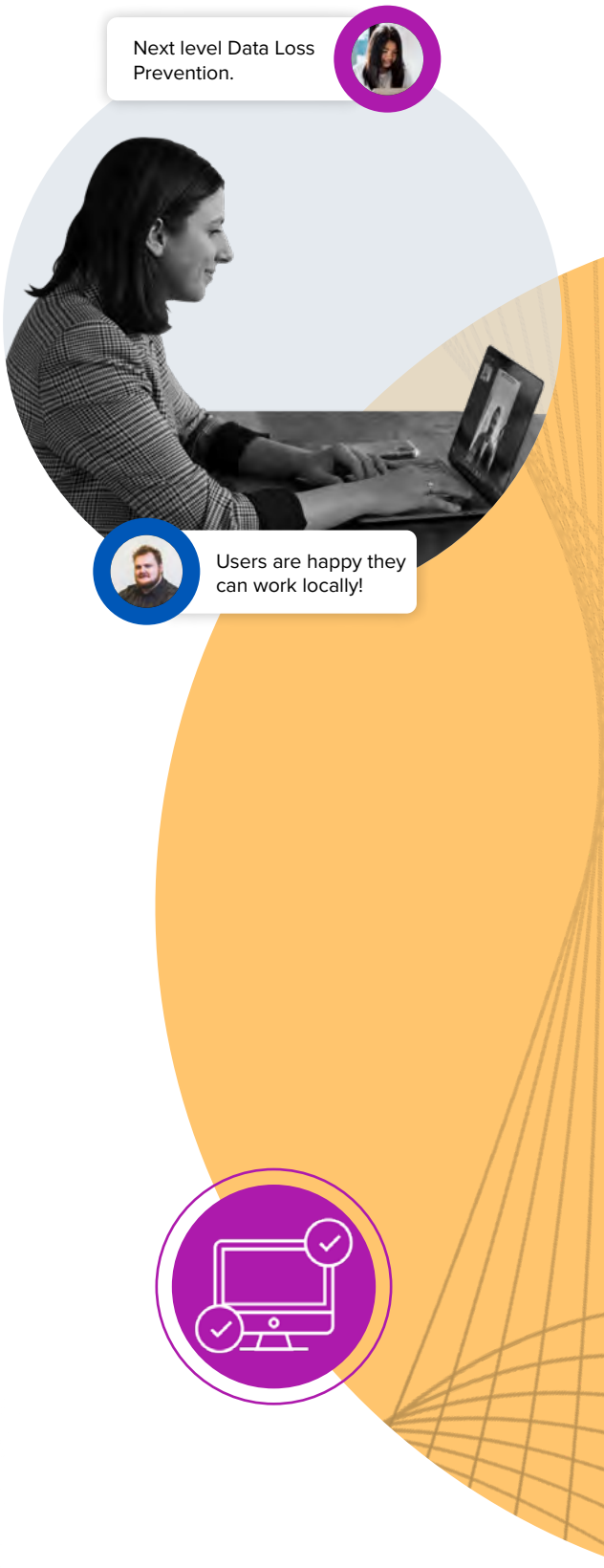
Introducing Venn

The Industry's First Virtual Desktop Alternative

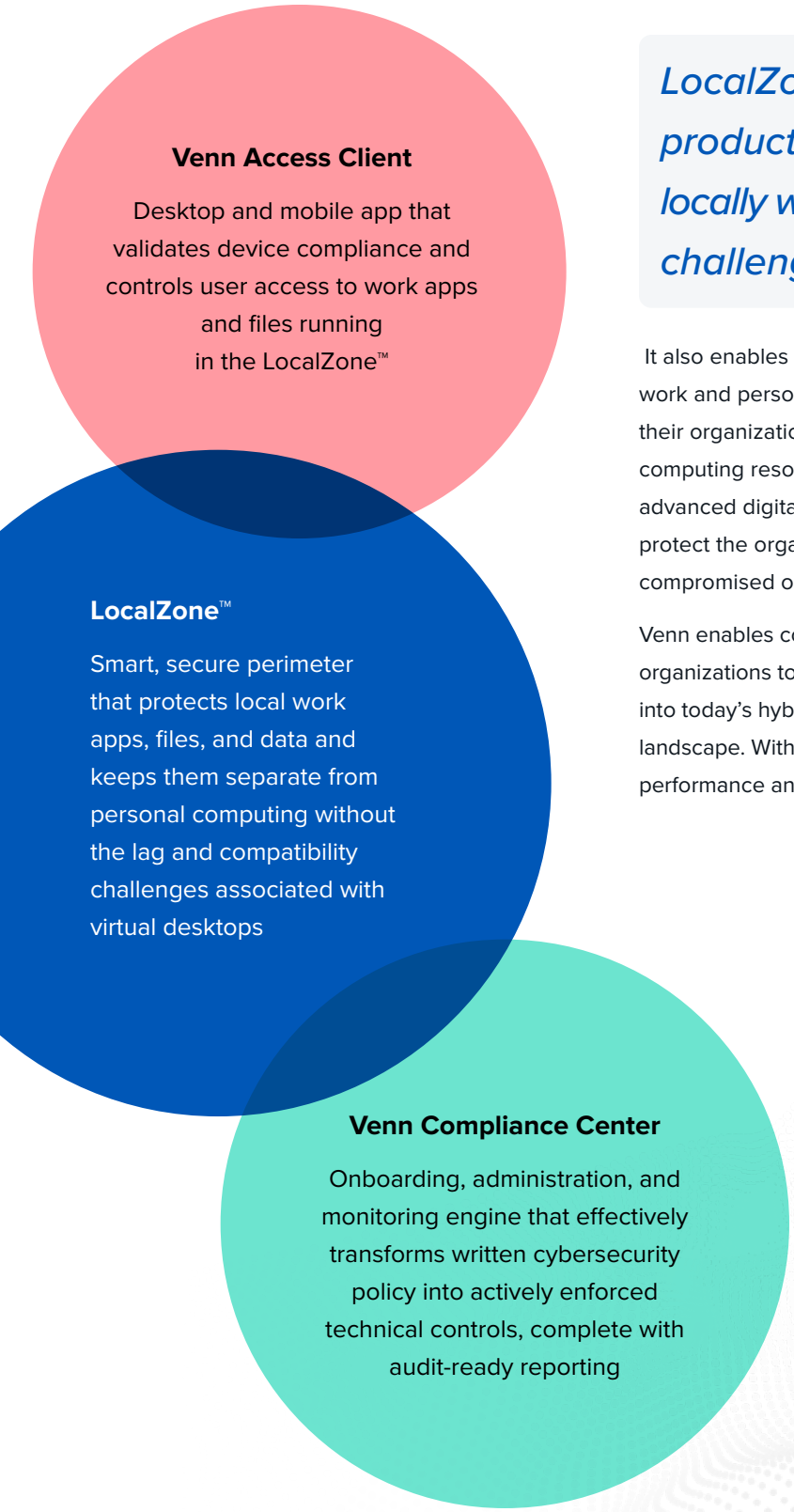
The Venn® Zero Trust Platform (ZTP) is the industry's first Virtual Desktop Alternative (VDA) that delivers the centralized management and critical information security benefits of legacy Virtual Desktop Infrastructure (VDI) along with additional essential cybersecurity capabilities that are not a part of standard VDI offerings. The platform does this without any dependence on or need for either a traditional on-premises VDI or cloud-hosted Desktop-as-a-Service (DaaS) solution. Instead, Venn directly 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).

Venn's core technology is LocalZone™, a smart, secure perimeter created around work applications and data that enables users to work locally with sensitive information.

Not a client hypervisor or an open-source container, LocalZone™ is a breakthrough technology that separates work applications, files and data from personal computing resources on the same device. Through patented application, filesystem and network isolation techniques, LocalZone™ enables work applications, files and data to safely and securely co-exist alongside a user's personal digital assets. LocalZone™ technology 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



LocalZone™ unlocks a new level of productivity by allowing users to work locally with none of the lag or compatibility challenges introduced by 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. Finally, through its advanced digital leakage/loss and filesystem capabilities, LocalZone™ can protect the organization's digital assets even when passwords have been compromised or malware protection fails.

Venn enables companies in regulated industries or any security-minded organizations 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.

venn

Venn Zero Trust Platform (ZTP) Principles

The Venn Zero Trust Platform (ZTP) is designed to ensure that work applications, files and data are only accessible in the LocalZone™ and that they are always separated from personal computing resources, protected from leakage, cyber-attack or accidental loss, and audited for compliance and/or regulatory purposes.

THE PLATFORM DOES THIS BY ADHERING TO SEVERAL CORE PRINCIPLES:

- **Separate work and personal applications, files, and data on BYO devices**
- **Use policies to prevent intentional or unintentional work data exfiltration or loss**
- **Maximize employee productivity without compromising work data security or compliance**
- **Protect work-related network traffic without impacting personal connectivity**
- **Protect privacy of personal applications, files, and data**
- **Shield work apps, files and data from ransomware and zero-day vulnerabilities**

"Zero trust is a way of thinking, not a specific technology or architecture," says Gartner Distinguished VP Analyst Neil MacDonald. "It's really about zero implicit trust, as that's what we want to get rid of."[16]

SOURCE

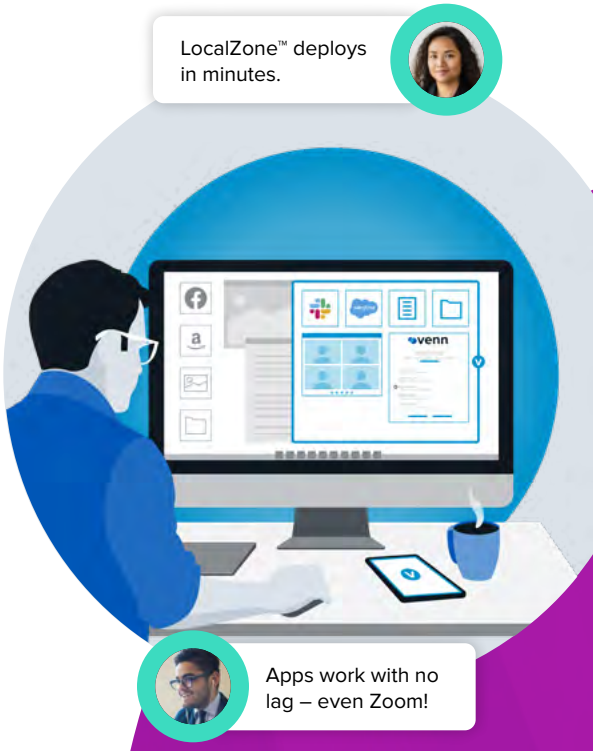
[16] https://www.gartner.com/smarterwithgartner/new-to-zero-trust-security-start-here/

LocalZone™

The Game Changer

LocalZone™ is patented technology that separates work applications, files and data from personal computing resources on the same device. LocalZone™ is 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, LocalZone™ does not virtualize the entire operating system. It also doesn't virtualize applications like Microsoft App-V or VMware ThinApp.

Through sophisticated and patented application, filesystem and network isolation techniques, LocalZone™ 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 or mobile device. This enables applications to run as intended, with responsive performance and none of the compatibility issues normally associated with VDI. LocalZone™ technology 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.



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.

venn

Are you ready to make the shift from legacy VDI to LocalZone™?

Book a demo with our experts and experience Venn's game-changing technology. We are excited to help you and your team stay productive, protected and private.

Connect with us today →

venn

Venn® is the industry's first Virtual Desktop Alternative (VDA) built for security-minded organizations. Venn introduces patented LocalZone™ technology that protects SaaS applications and data and delivers Zero Trust security with a 10X better user experience than legacy VDI. Over 700 organizations, including Fidelity, Guardian, and Voya, trust Venn to meet FINRA, SEC, NAIC, and SOC 2 standards.

VENN.COM