eBook:

WHY NOW IS THE TIME TO RE-THINK DESKTOP DELIVERY

Cloud@Work™

Today's Business Imperatives:

Zero downtime is a must.

We need **modern solutions** that help us **work together more efficiently.**

Our team works from many locations. We need to **stay connected no matter what.**

We need **anywhere and anytime access** to files and business tools to **serve our customers** and **stay competitive**.

Our **data has to be secure**. I need to know my company **is protected from viruses, malware, theft**, etc.

We need **better tools to stay connected.**

Introduction

To create and support modern work, organizations like yours are likely dealing with hybrid work scenarios, raising questions like:

- How do you accommodate a distributed workforce?
- How do you onboard new employees, some of which are fully remote?
- How do you ensure that the devices accessing corporate resources are secure and uncompromised?

Whether SaaS, hosted, or on-premises, workers need devices to access ERP and other business-critical applications and data, but supplying devices to a diverse and distributed workforce has become cost-prohibitive and increasingly challenging to support. Organizations are struggling to ensure security, compatibility, performance, and reliability of the devices, along with managing costs, updates, and technical support.

To enable productivity and ensure maximum security and performance, organizations are re-thinking their traditional desktop delivery strategy and evaluating cloud-hosted desktops as a future-proof solution.

As you'll learn in this e-book, a cloud-hosted desktop service helps to enable hybrid work, keeps company resources secure, and eases the burden on IT departments—all while taking advantage of existing resources and maintaining productivity.

The pandemic accelerated innovation or digital transformation

55%

Employees are high performers when provided radical flexibility over where, when and with whom they work versus 36% of those working 9 to 5 in the office.[1]

65%

IT employees noted in a 2021 Gartner survey, that whether they can work flexibly will impact their decision to stay at the organization.[2]

Modern Work

When talking about the changing work environment, specialists, particularly those in the IT field, are using the term *modern workplace*. If you're not familiar with that term, in short, it's a workplace that supports everyone's individual ways of working by utilizing different digital solutions that are flexible enough to adapt to constantly changing employee and enterprise needs – like the demand for hybrid or remote work.

Organizations around the world are quickly pivoting in three key areas:

- Making arrangements to permanently support hybrid work;
- Adapting technologies to support productivity and collaboration for a distributed workforce; and,
- Deepening investments in cybersecurity as threats continue to increase and evolve.

Remote work is an increasingly common paradigm, but traditional IT security approaches have long been perimeter-based, meaning they were primarily concerned with what happens inside of the office and the corporate network.

When users perform their job duties from remote locations such as a home office or airport lounge, the potential security threats increase, because people are accessing corporate data and systems from outside of the corporate perimeter.

With 98% of workers wanting to work remotely at least some of the time, it's essential that organizations adapt their IT strategy accordingly.

32.6M

By 2025, it's estimated that 22% of full-time workers in America will be fully remote (an 87% increase from pre-pandemic levels.)[3]

44%

C-levels say they have reduced office space or plan to as a result of hybrid and remote working.[4]

$10-14K

Estimated annual expenses for full-time, in-office workers (commuting, meals, and pet care for those with pets).

Working remotely 3.3 days/week, cuts this expense in half.[5]

16%

Companies that are now fully remote, operating without a physical office.[3]

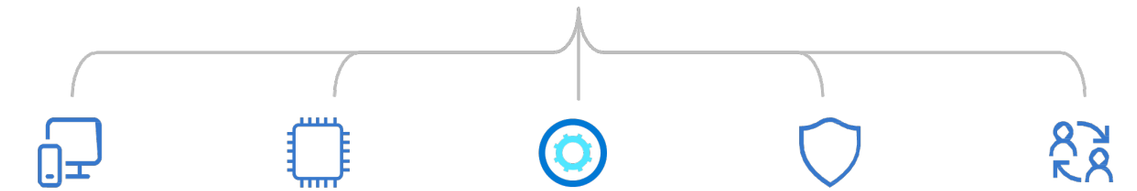
End-User Computing

The business and IT challenges associated with deploying and supporting corporate issued laptops for remote workers are manifold and complex. Some of the main challenges include:

- Ensuring the security and compliance of the laptops and the data stored on them, especially when they are used in unsecured networks or locations.
- Providing adequate technical support and troubleshooting for the remote workers, who may face issues such as connectivity problems, software updates, hardware failures, or malware infections.
- Managing the inventory and lifecycle of the laptops, including procurement, distribution, maintenance, replacement, and disposal.
- Balancing the cost and performance of the laptops, as well as the bandwidth and storage requirements for the remote workers.
- Enhancing the productivity and collaboration of the remote workers, who may need access to various applications, tools, and resources that are hosted on the corporate network or cloud.

Remote and hybrid work has compelled companies around the world to rethink how they manage and secure employee devices.

The five components of the end user computing experience



Devices
that meet specific job requirements

Operating system
that's easy to manage, update, and use

Management
solutions for a heterogenous device estate that includes personal devices

Endpoint security
that defends against cyberattacks without disrupting productivity

Collaborative apps
that work across all devices, for each user

1-in-10

10% of laptops are likely to be stolen within the first 12 months of purchase. 90% will never be recovered.[6]

End-User Computing: Security

Computing devices are vulnerable to cyberattacks, malware, viruses, data breaches, theft. They require constant security updates and patches, antivirus software, firewalls, encryption, and passwords to protect them from external threats. Users also need to be careful about phishing emails, malicious links, or downloads that can compromise their devices.

Cyber-attacks are more sophisticated and constantly evolving

Security Challenges

- Security teams constrained by the growing sophistication and damaging impacts of cyberattacks
- Larger surface area resulting from distrusted workforce and increase in devices, requires greater understanding of gaps and vulnerabilities
- Mix of on-premises and cloud tools creating more complexity
- Supporting a Bring-Your-Own-Device (BYOD) policy
- Expanding data regulations and associated compliance requirements

95%

Cybersecurity breaches that can be traced to human error.[7]

16%

IT Professionals seeing an increase in non-approved devices accessing network resources.[4]

$1.07 M

Average increase in cost of a breach when remote work is a factor in causing a data breach.[8]

End-User Computing: Management

Physical computers for end users are difficult to manage and monitor – more so when workers are working from any device and in any location. They require individual installation, configuration, troubleshooting, and support for each device and user. They also pose challenges for compliance and standardization across the organization. It's not surprising that 67 percent of IT professionals feel overwhelmed by trying to manage diverse endpoints across various hybrid work scenarios.[11]

New devices and workstyles drop new burdens on IT's shoulders

Management Challenges

- Need to deploy devices and onboard new employees whether in-office or remote
- IT teams hampered by multiple tools and limited visibility over device estates
- Keeping up with adoption of new apps technology for monitoring remote workers
- Handling endpoint diversity with BYOD

73%

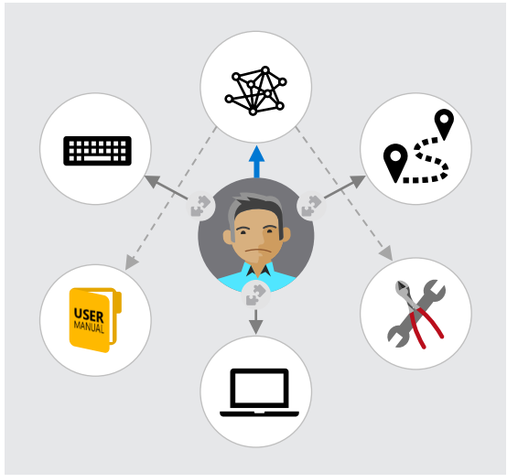
Increase in IT workloads in response to hybrid and remote work.[4]

67%

IT Professionals seeing feeling overwhelmed trying to manage diverse endpoints across various hybrid work scenarios.[9]

26%

Experiencing an uptick in Shadow IT based on a 2022 survey by Ivanti.[4]



End-User Computing: Cost Savings

Physical end user computers are expensive to purchase and maintain. They require regular updates, repairs, replacements, and backups, which can add up to the total cost of ownership. Depending on the environment and available resources, the device may need to be shipped on multiple occasions adding to the expense and putting it at risk for being damaged or lost. While attempting to address the costs associated with devices, business leaders must ensure that are appropriately investing in data security.

An uncertain economy dictates a need for continuous agility and cost savings

Cost Optimization Challenges

- An uncertain economic future requires continuous agility and cost savings
- Investing in tools to ensure end user experiences no matter where work is performed
- Meeting business requirements to scale securely in the most cost-efficient manner
- Supporting end users to remain productive with constrained IT resources
- Employees are also struggling to manage expenses and are attempting to find ways to save.

"Organizations that maintain a focus on agility while cutting costs will emerge leaner, more capable, and better poised to respond to future demands."[10]

80%

Surveyed workers say that they'd rather have separate personal and work devices. Namely due to concerns over their privacy.[11]

67%

Hybrid and remote workers would expect a pay increase to make up for additional costs if no longer able to work remotely. If mandated to work in-office, 46% would "quiet quit."[12]

Data: Leakage

Data leak occurs when data is left accessible and unprotected. Data leakage can have serious consequences for organizations, such as reputational damage, legal liability, regulatory fines, loss of competitive advantage, and breach of trust with customers and partners.
Some of the common causes of data leakage in a hybrid or remote work environment are:

- **Lack of proper encryption and authentication for data in transit and at rest.** Data that is transmitted or stored on unsecured networks, devices, or cloud services can be easily intercepted, stolen, or tampered with by hackers or malicious insiders.
- **Use of personal devices or accounts for work purposes.** BYOD or personal accounts may not have adequate security measures, such as antivirus software, firewalls, password protection, or biometric authentication. They may also expose the data to other apps or services that have access to their device or account, such as social media platforms, email providers, or cloud storage providers.
- **Lack of visibility and control over data access and usage.** Organizations that do not have a centralized and comprehensive data governance framework may not be able to monitor and audit the data access and usage activities of their employees, contractors, vendors, or partners. They may also not be able to enforce data security policies and standards across different devices, platforms, and locations.

Whether in-office or remote, a lack of awareness and training on data security best practices can also lead to loss of data.

25 Million

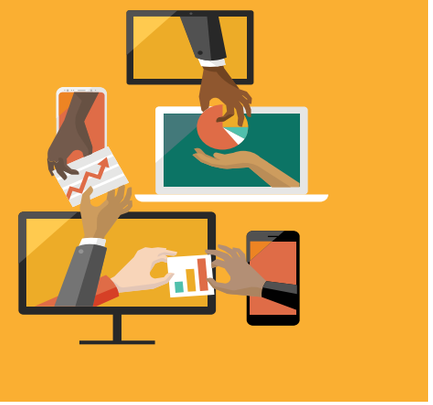
VPN User Records Were Exposed in 2022 (and 21 million the year before) proving that VPNs provide a false sense of security.

26%

Workers report being tempted to make copies of important company data as a precaution in they lose their job or the company becomes insolvent.[13]

17%

Employees do not tell their IT department when they're using their own device for work. This is true whether or not their employer has a BYOD policy.[11]



Data: Security

As cybersecurity threats continue to evolve and become more sophisticated, enterprise IT must remain vigilant when it comes to protecting their data and networks.

Common threats an organization's data include:

- **Insider Threat** – authorized user intentionally or unintentionally misuses network access, negatively affecting critical data or systems.
- **Viruses and worms** - malicious software programs (malware) aimed at destroying an organization's systems, data and network.
- **Botnets** - malware searches for vulnerable devices across the internet, aimed to destroy an organization's systems, data and network.
- **Drive-by download** – malicious code is downloaded without a user's knowledge and without clicking on anything.
- **Phishing** – employs social engineering to trick users into breaking normal security practices and giving up confidential information.
- **Distributed denial-of-service (DDoS)** - compromised machines attack a target, e.g., server, website or network, making it inoperable.
- **Ransomware** – a computing environment is locked, typically by encryption, keeping the victim from accessing data on it.
- **Exploit kit** - a programming tool that enables a person without any coding experience, create, customize and distribute malware.
- **Advanced persistent threat (APT)** - an intruder penetrates a network and remains undetected for an extended period of time.
- **Malvertising** - technique used to inject malicious code into legitimate online advertising networks and web pages.

It's necessary to ensure that end users and any device that they use to access a network resources, strictly adhere to an organization's data security policy.

0%

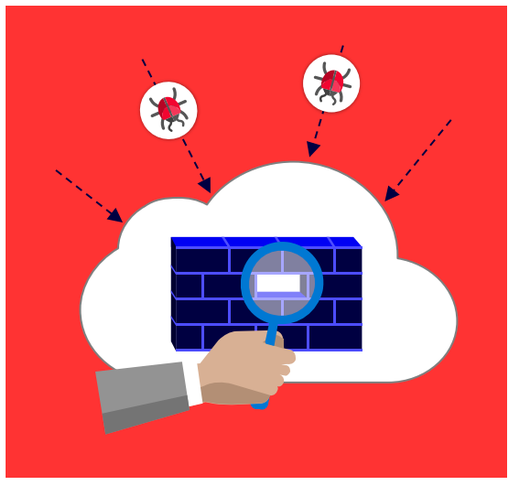
Unemployment rate for cybersecurity professionals.[14]

60%

Companies that have experienced 30 or more cyber incidents within a single year.[15]

2,200/day

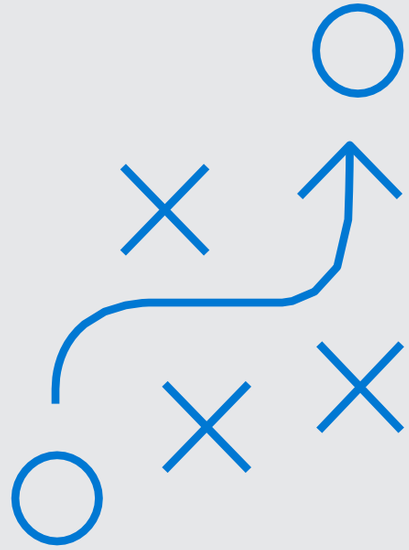
Internal security breaches encountered by American businesses.[16]



Re-think Desktop Delivery

Whether in-office, hybrid, or fully remote, cloud-based desktops can empower your workforce, maximize IT investments, and help to secure sensitive date. Through virtualization, employees can use just about any device to utilize a secure and centrally governed system to access all the compute power, data, and applications needed for productivity and collaboration.

Unlike traditional desktop delivery for hybrid workers, cloud-desktops are centrally governed making security, availability, and performance easy to manage.



Cost Savings

Shift from CapEx to an OpEx model, while reducing or eliminating the cost and complexity of buying, managing, and shipping company-owned devices.

Built-in security

Protect sensitive data from accidental or malicious exfiltration, compromise, or loss via data centralization and a reduced threat surface.

Rapid Onboarding

Onboard (and offboard) in minutes and depending on your device policy, there may be no equipment to send or return.

Control

Shift from CapEx to an OpEx model, while reducing or eliminating the cost and complexity of buying, managing, and shipping company-owned devices.

Convenience & Privacy

Enables worker locally on a single device with clear separation between work use and personal use.

Resiliency

Help ensure continuity and access for your workforce and company data even in the most challenging circumstances.

Cloud at your Pace

Can be adopted at any phase of a digital transformation strategy.

Productivity

Enable efficiencies with anywhere, anytime, any device access for workers.

Sustainability

Reduce or eliminate the need for compliant data destruction of decommissioned hard drives.

With virtual desktops, data never resides on a physical device and policies control drive mapping, restrict downloads, disable clipboard mapping, and enable watermarks.

Desktop Virtualization for ERP-centric Organizations

Virtualization is helping organizations address many business needs around flexibility, security, compliance, and employee-specific requirements. However, deploying and managing an on-premises virtualization infrastructure, especially for desktop scenarios, can be complex and costly for IT and the business. Additionally, it requires deep experience with skills that may not currently exist within the organization.

For organizations interested in virtual desktops but unprepared to setup and manage the infrastructure, there are numerous service providers that offer options for hosting and managing. The options can range from one-size-fits-most desktops to highly customized, business-specific solutions and as such, cost, performance, and security will vary.

For an organizations with an ERP system, selecting a virtual desktop service provider with solutions designed specifically for ERP-centric businesses provides the greatest opportunity for an ideal solution, smooth migration, and on-going success.

1. Gartner® Insights, "Future of Work," October 2022.
2. Gartner, 2022 Leadership Vision for Chief Information Officers.
3. Upwork, 2nd annual Future Workforce Pulse Report," 2021.
4. Ivanti Report, "Defending IT Talent," Q12023.
5. Global Workplace Analytics, "State of Remote Work," 2022.
6. FBI Internet Crime Report, 2020
7. World Economic Forum, Cyber Risk Study, 2020
8. IBM, "2023 Cost of a Data Breach Report," 2023.
9. JumpCloud, "IT Trends Report: Remote Work Drives Priorities in 2021," 2021.
10. PwC, "Agile Defense: Sustainable Cost Reduction on the Path to Greater Agility," 2014.
11. Zippia, "BYOD Trends in the Workplace," October 2022.
12. Owl Labs, 2023 State of Hybrid Work," 2023.
13. DataBasix, "Statistics Of Cyber Security Risks When Working from Home, 2020.
14. Cybercrime Magazine, Cybersecurity Jobs Report, April 2023.
15. Ponemon Institute, 2021.
16. Techjury Research "Internal Threat," 2022.

Support *modern work* with a purpose-built desktop solution

Cloud at Work's solutions are designed and developed specifically to meet the demands of ERP-centric businesses.

For organizations with a Hosted or Next-Gen ERP solution, *DaaS at Work* provides hybrid workers with an agile, high-performance desktop that safeguards access to applications, sensitive data, and networked resources. As a managed Desktop-as-a-Service (DaaS) solution, Cloud at Work delivers virtual desktops to end users over the Internet, licensed with a per-user subscription.

Cloud at Work™

Highlights:

- Platform is built and managed by Cloud at Work with support included at no additional cost.
- Using any internet-enabled device, users access Apps and internal resources at LAN speeds.
- Legacy Sage applications can be hosted in Cloud at Work's Virtual Private Cloud (VPC) or in Azure and then accessed through *DaaS at Work*.

CONTACT US TODAY TO LEARN MORE.

info@thecloudatwork.com | (800) 719-3307 | thecloudatwork.com