Can cloud-client computing rescue hybrid work?

Contents

Over the last several hundred years, there have been a few key moments where the trajectory of the workplace changed dramatically. Among the biggest of these shifts were the Industrial Revolutions of the 1800s; World War 2 when more women began to join the workforce; the 1990s with the introduction of PCs and the internet; and the 2020 COVID-19 pandemic, which ushered in a new era of hybrid work.

This shift toward hybrid work happened so quickly that many organizations didn't have time to approach it as strategically as they might have liked. As a result, many organizations have implemented hybrid work, but haven't yet optimized it.

The rapid shift to remote and hybrid work

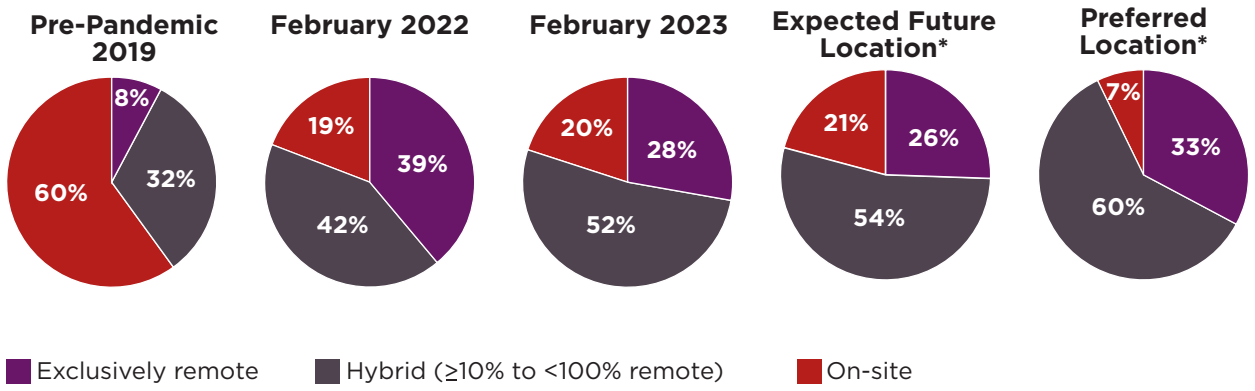
Gallup's research on hybrid work has shown that, before the pandemic, on-site work was by far the most common paradigm. In 2019, 60% of workers with remote-capable jobs still worked on site, while only 8% were fully remote. Today, hybrid and remote work are more prevalent and preferred among workers with these types of roles.

The rise of the new hybrid work model has been supported by the simultaneous proliferation of cloud-based business applications and services, such as Microsoft 365, which was first announced in 2017. The pandemic accelerated cloud adoption for 91 percent of enterprises, who needed to provide employees remote access to company data and applications. Cloud data centers now process at least 95 percent of all workloads.

Work locations for remote-capable jobs

Before the pandemic, on-site work was the most common paradigm, even for workers with remote-capable jobs. Today, hybrid and remote work are prevalent and preferred among workers with these types of roles.

Work locations for remote-capable jobs among U.S. employees



*As of February 2023
Note: Due to rounding, totals may not sum to 100%
Source: Gallup Indicators: Hybrid Work

As companies settle into the new hybrid work paradigm, there are still more opportunities to unlock, including for securing and managing endpoints that are working remotely. Important new advancements in cloud-client computing are offering companies the ability to further optimize hybrid work at scale, particularly by taking advantage of purpose-built solutions for the cloud.

In this whitepaper, we'll discuss how modern cloud-client computing — deployed on standard PCs — using a next-gen operating system (OS) that's purpose-built for the cloud can pave the way for a hybrid workplace that is easier for teams to manage and is more secure, cost-effective and eco-friendly, without compromising the end user experience and productivity.

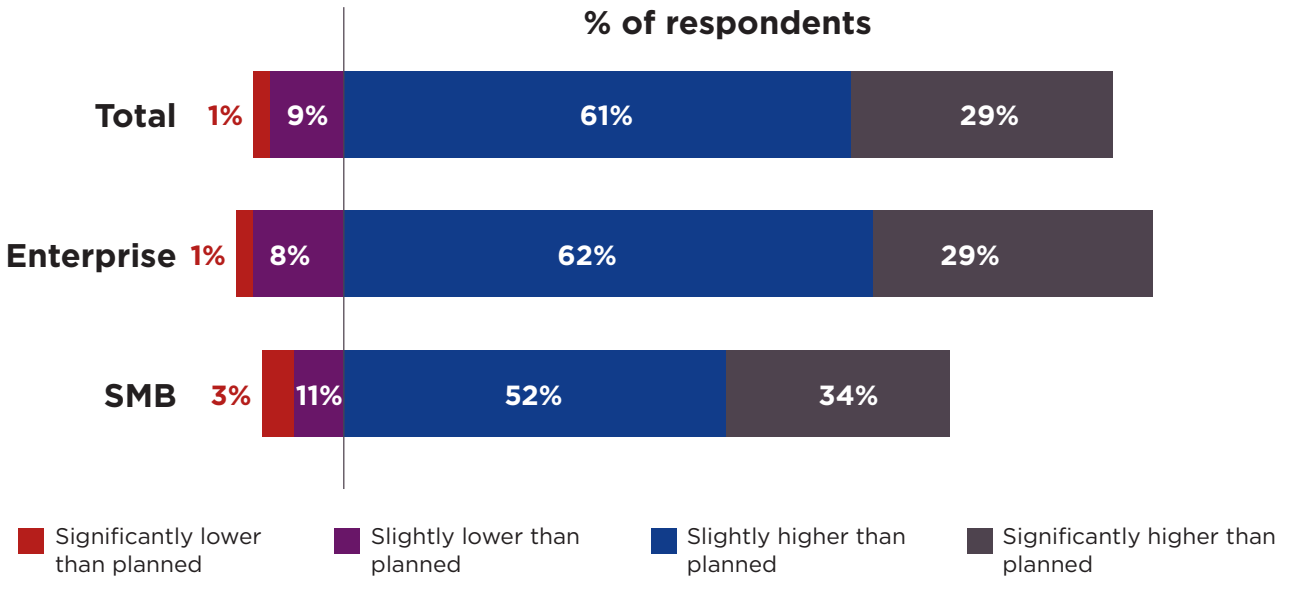
COVID-19 accelerated cloud adoption

Although many organizations were moving to the cloud prior to the pandemic, they were forced to quickly accelerate their cloud adoption to enable remote work.

By 2021, 9 out of 10 enterprises said COVID-19 had pushed their cloud usage slightly or significantly higher than initially planned.

Cloud data centers processed 95% of all workloads in 2021.

Change from planned cloud usage due to COVID-19



Sources: InfoWorld: The COVID pandemic's lasting impact on cloud usage; Cisco: Global Cloud Index Projects Cloud Traffic to Represent 95 Percent of Total Data Center Traffic by 2021; Flexera 2023 State of the Cloud Report

Virtual desktops go mainstream

If this surge in remote and hybrid work had happened just a few years sooner, technology would not have been ready for it. But thanks to the proliferation of cloud-based infrastructure and applications in the 2010s, organizations were able to quickly purchase and implement the tools they needed to enable a fully remote workforce.

When organizations chose to shift to a cloud-first model — where their mission-critical data and applications were stored in the cloud — many required employees to access those systems through a secure, virtual desktop environment. This was a simple solution for enabling employees to work from anywhere while limiting the amount of company data employees had to store on their devices.

Virtual desktop infrastructure (VDI) has been around for decades but was typically used in the workplace to connect employees who were using thin or zero clients — read-only devices with limited or no connectivity and restricted use cases focused on task-based workloads. In an attempt to simplify management and increase security, IT centrally managed the resources, applications, data and OS from a datacenter.

The purpose was usually to lock down security risks, but it also restricted what workers could do on their devices. That was a benefit, not a drawback, for organizations in highly regulated fields like healthcare or financial services, where human error could threaten the exposure of the sensitive data of hundreds or thousands of people.

Today, VDI usage is on the rise across a variety of industries. More than half of enterprises are now using VDI, and the desktop virtualization market is projected to reach $18.9 billion USD by 2026.

However, many of the organizations that began using VDI at scale in 2020 are not using thin clients. They have invested in traditional laptops and mobile devices or are allowing employees to use their personal devices to access VDI over their home internet.

The rise of virtual desktops

Today, virtual desktop usage is rising sharply, thanks in large part to the growth of cloud-based services and applications.

$10.6

billion USD was the global market estimate for desktop virtualization in the year 2020. It is projected to reach $18.9 billion USD by 2026.

52%

of enterprises are using virtual desktop infrastructure as of 2023.

68%

growth occurred in the Desktop-as-a-Service market between 2018 to 2022, from $3 million USD to $5.6 million USD. It is forecast to reach $34.9 million USD by 2033.

Source: BusinessWire: Insights on the Desktop Virtualization Global Market to 2026; Spiceworks: The 2023 State of IT; Future Market Insights: Desktop-as-a-Service Outlook

The evolution of cloud-client computing

Before exploring the benefits of using a next-generation OS to facilitate a cloud-client computing model, it's important to understand that cloud-client computing has evolved beyond its historical limitations:

- **Expanded functionality:** In the past, cloud-client computing offered limited functionality and narrow use cases. However, the next-gen OS can support today's resource-intensive collaboration tools, delivering a positive user experience in addition to security and ease of management.
- **Reduced cost:** An increase in cloud-client computing was historically associated with over-provisioned data centers that required an increased IT support organization to build, deliver and manage the virtual workloads. However, today's next-gen OS can operate on standard laptops and other mobile devices, eliminating the need for investment in thin clients. It is also purpose built to connect with the cloud — no on-site data center required.
- **Simplicity:** IT teams who have never managed a cloud-client computing program need not be intimidated by the potential learning curve. The next-gen OS greatly reduces the effort involved with adopting a new endpoint model.

In short, the next-gen OS is purpose-built to connect users to applications and desktops delivered via the cloud. It supports not only commonly used peripherals, like webcams, headsets and printers, but also virtual desktop infrastructure (VDI) agents, cloud storage and the cloud-client computing model — giving IT teams the ability to instantly turn any device into a hybrid workstation of the future.

How a next-gen OS can optimize hybrid work at scale

Strategic IT teams are recognizing there are more optimal ways to manage a large hybrid workforce. VDI was a great first step, but the next step is to drive better performance and efficiency at the endpoint by installing an OS that's purpose-built for VDI.

Here's what to consider when implementing a next-gen OS:

1. Provides secure management at scale

The heaviest burdens of the hybrid workplace fall on organizations' IT teams who are tasked with managing thousands of endpoints without having physical access to them. With a next-gen OS, one IT person can easily manage tens of thousands of endpoints, finally taking full advantage of the centralized management afforded by virtualization.

— Centralized patching and updates

Patch management can be an ongoing struggle for busy IT teams, especially when they must manage updates and patches for thousands of company endpoints. On average, it takes organizations 65 days to remediate critical severity vulnerabilities. Unfortunately, unpatched vulnerabilities can be disastrous for companies.

However, when an organization is using a next-gen OS, they can patch and update one centrally managed, cloud-based Windows implementation. The next-gen endpoint OS and the applications on it can be patched or updated independently and seamlessly from a central location without the need for additional software like a virtual private network (VPN). Employees then automatically access the secure, updated version when they sign in, reducing vulnerabilities and downtime.

Patch management is critical and challenging

Although patch management is one of the most important security measures organizations can take, many struggle to stay on top of it.

33%

of all vulnerabilities are either high or critical severity.

90%

of common vulnerabilities and exposures can be exploited by hackers with limited technical skills.

65

days is the average time it takes organizations to remediate critical severity vulnerabilities.

Unpatched vulnerabilities are the most prominent attack vector for ransomware.

Sources: PR Newswire: Edgescan Releases 2023 Vulnerability Statistics Report Revealing 33% of Vulnerabilities Discovered in 2022 were High or Critical Severity; Business Wire: Ransomware 2021 Year End Report Reveals Hackers are Increasingly Targeting Zero-Day Vulnerabilities and Supply Chain Networks for Maximum Impact; Redscan: Redscan analysis of NIST NVD reveals record number of vulnerabilities in 2021

— Secure remote access and management

IT teams with hybrid workforces often use VPNs to enable employees to securely connect to company systems, to manage remote endpoints and to configure the applicable networks for remote access. VPNs can often be eliminated as a cost center by switching to a next-gen OS.

A next-gen OS enables secure and effective management of end-user devices outside the corporate network without requiring a VPN solution. It acts as a virtual tunnel, supporting secure and encrypted two-way communications based on open communication standards like TLS/SSL encryption and WebSocket protocol. Two-way communications between endpoints and the management infrastructure are encrypted and secure, even when traveling across insecure zones. Further, a next-gen OS can simplify network configuration by minimizing the limitations posed by Network Address Translation (NAT) technology.

— Read-only OS

Cyber threats are constantly evolving. Today, organizations encounter an array of security challenges at the edge, which is the network's most exposed point. These challenges converge to form a "perfect storm" of potential threats to endpoints that must be dealt with. Some of these challenges have been present for decades, while others are more recent. For example, the practice of the hybrid workplace is extending the corporate network into employees' home offices or living rooms, presenting new vulnerabilities. Other challenges include sophisticated malware, such as ransomware and keyloggers; the need for endpoint security and patching; and the rising expectations for user experience.

By deploying a next-gen operating system, companies can benefit from increased security measures that protect against accidental or malicious downloading of malware by employees. The read-only and modular design of this OS reduces its vulnerability to attacks and unauthorized modifications, making it highly resistant to tampering and malware. This results in a strong security posture that helps to reduce risks and protect sensitive information.

In addition, implementing a read-only OS allows organizations to simplify their security infrastructure by reducing the need for multiple third-party solutions and agents. This consolidation streamlines security operations and minimizes potential vulnerabilities that can arise from managing multiple software components.

Endpoint attacks are prevalent and harmful

Ransomware and other endpoint attacks rose as more workers went remote. Using a read-only OS significantly reduces risk exposure at the endpoint.

68%

of organizations have experienced one or more endpoint attacks that successfully compromised data and/or their IT infrastruction.

68%

of IT professionals found that the frequency of endpoint attacks had increased since the year before.

64%

of organizations experienced ransomware infections in 2022.

2022 was the second-worst year ever for ransomware attack volume, behind only 2021.

Sources: CRN: Ransomware Attacks Plunged 48 Percent In US Last Year: SonicWall

2. Maximizes hardware investments

Today's hybrid workforce requires reliable access to devices that enable them to be productive from their first day on the job to the last. A next-gen OS can provide time and cost-saving benefits throughout the lifecycle of any device, giving IT teams the ability to refocus those resources elsewhere.

— Faster onboarding

When a new device is purchased — either as a replacement for an existing employee device or for onboarding a new hire — the typical organization with a hybrid workforce will have the device shipped from the factory to the company's IT department, where the IT team will set up the device, set up the right policy and profile, download the right applications for that user's role and ship the device to the user. The user will then speak with IT to connect to the appropriate virtual environments so they can start working. This process may take weeks from end to end.

With a next-gen OS, the IT team can order the user's new device with the OS pre-installed. The factory can ship the device directly to the employee, who enters their password to log in to their virtual workspace — effectively bypassing IT in this process, reducing cost and improving the user experience for everyone involved. If additional training or support is needed, the IT team can use the OS's secure shadowing functionality to temporarily take remote control of the new device and help the employee resolve their issue without the need to install third-party solutions like a VPN, solving additional challenges associated with supporting devices when an employee is not in the office. This process can take place as soon as the day after a new device is purchased, using overnight shipping from the manufacturer, creating important productivity gains for the IT team and device recipient alike.

— Extends the battery and total life cycle of devices

Today's IT teams are increasingly focused on reducing capital expenses (CapEx) and opting for "as-a-service" operating expense (OpEx) delivery models for everything from data storage to virtual desktops. But while it is possible to lease laptops and other hardware, many organizations still prefer to purchase these items outright to maximize their value. Of course, technology has a lifespan. As a result, organizations with thousands of endpoints must allocate a portion of their budget each month to replacing devices as they become outdated or less functional.

Leveraging a next-gen OS delivers significant cost-saving benefits that free up CapEx budget that can then be used for other technology purchases. In some cases, a next-gen OS is lightweight enough to repurpose older or less powerful endpoints, extending the life of devices and reducing e-waste. However, depending on the use-cases in question, the device still needs to be powerful enough to run the applications.

Due to the inherent security advantages of a read-only OS, organizations can reduce their expenses while maintaining robust protection by eliminating the need for tool proliferation. Using a read-only OS reduces the need for many third-party solutions and agents, which can be costly to acquire, maintain and integrate.

Moreover, the lightweight OS requires less power consumption, increasing the daily battery life of a device. IT teams can reallocate any money they save toward extended warranties and device analytics software, further extending the life of their devices.

3. Delivers a seamless user experience

Providing a digital workspace that meets both security and user experience needs is a delicate balancing act. With the shift to hybrid work, IT and users face new technological challenges. A solution designed for a connected world is required. Prioritizing the user experience does not mean sacrificing security or ease of management.

— Reduced network traffic

Collaboration and productivity software is essential to the hybrid workforce, with more than 80% of workers using collaboration tools today, as opposed to just over half of workers in 2019. At the same time, the GPU requirements for productivity applications have more than doubled, creating special considerations for IT teams who want to ensure workers have a seamless experience when accessing these applications in the cloud.

An elastic, next-gen OS can help organizations get the maximum performance from their productivity and collaboration applications by taking advantage of available protocols or using purpose-built agents that intelligently redirect how and where to render a particular application or even redirect what peripherals to use locally on the endpoint. A next-gen OS can ensure that, regardless of the cloud provider, resource-intensive applications running in the cloud can offload the heavy processing load to the local endpoint, which relieves the host of that burden allowing more virtual desktops to reside on it. This has the added benefit of increasing the host density and can decrease the cost of each virtual desktop.

Another factor that can shape the user experience is the management of call or video data. When this data is sent back and forth to the cloud (hairpinning), it results in a notable impact on network traffic and, in turn, the end-user experience. However, by directly redirecting audio and video to the intended recipients, the need for hairpinning is minimized. The presence of these protocol optimizations, combined with comprehensive compatibility with a wide range of headsets and peripherals, enhances the attractiveness of transitioning to a purpose-built cloud client.

The growth of productivity and collaboration software

Collaboration and productivity software are the lifeblood of the hybrid workforce. An elastic, hardware-software OS can help organizations get maximum performance from their productivity and collaboration applications.

The GPU requirements for productivity apps have **more than doubled** between 2015 to 2020.

Almost **80% of workers were using collaboration tools** for work as of 2021, up from just over half of workers in 2019.

Source: Gartner Survey Reveals a 44% Rise in Workers' Use of Collaboration Tools Since 2019; Forbes: The 3 Reasons Why Enterprises Accelerate Their Virtual Desktop Infrastructure (VDI)

The next-gen OS is here to rescue hybrid work

Hybrid work is going to remain the dominant workplace model for the foreseeable future. For IT teams to thrive in this paradigm, it's vital they optimize their endpoint strategy based on the realities of the new, cloud-first world.

For an endpoint strategy to coincide with an organization's cloud strategy, it must enable users and solutions to take advantage of the innovations and unleash the potential of the workforce without compromising on security or management at the edge.

Installing a next-gen OS that's purpose-built for the cloud is a simple, cost-effective way to improve security, maximize device investments and deliver a good user experience to employees who are using virtual desktops. This once-niche computing model is poised to see a meteoric rise in the coming years — and strategic IT teams who lead the charge can start reaping the benefits today.

Lenovo powered by IGEL is the ultimate cloud-client device

Lenovo powered by IGEL provides the ultimate cloud-connected device, purpose-built for VDI, Desktop-as-a-Service (DaaS) and Digital Workspaces. Together, we offer a simple and secure solution that supports the mission-critical functionality and demands of enterprises and other organizations' evolving environments.

Has your company reviewed IGEL as part of your endpoint strategy? Learn more and schedule your meeting today, **click here**.

About Lenovo

Lenovo (HKSE: 992) (ADR: LNVGY) is a US$62 billion revenue global technology powerhouse, ranked #171 in the Fortune Global 500, employing 77,000 people around the world, and serving millions of customers every day in 180 markets. Focused on a bold vision to deliver smarter technology for all, Lenovo has built on its success as the world's largest PC company by further expanding into growth areas that fuel the advancement of 'New IT' technologies (client, edge, cloud, network and intelligence) including server, storage, mobile, software, solutions, and services. This transformation together with Lenovo's world-changing innovation is building a more inclusive, trustworthy, and smarter future for everyone, everywhere. To find out more visit **https://www.lenovo.com**, and read about the latest news via our **StoryHub**.

About IGEL

Today, the world of work is hybrid. Multiple clouds can deliver applications sourced from anywhere to a widely distributed workforce using all types of devices. Right at the moment when the world of work needs it most, IGEL has the solution for fully managed, secure endpoint access to any digital workspace that gives IT teams strong control and end-users the freedom to work as they wish in a hybrid world. Enabling choice of any cloud, from any device, anywhere, IGEL unlocks a collaborative and productive end user computing experience while solving the common security and management challenges required to compete and win in today's world of hybrid work. With a growing ecosystem of more than 100 IGEL Ready technology partners, IGEL has offices in Europe and the United States and is represented by partners in over 50 countries. For more information on IGEL, visit **www.igel.com**.