Introduction

According to IDC's Future Enterprise Resiliency and Spending Survey, Wave 12 (January 2022), only 2% of companies don't expect to have a hybrid workforce in 2022. These hybrid workforces will require secure, equal access to enterprise resources, regardless of the client endpoint to which they have access.

Despite stellar growth in the traditional PC market (14.2% in 2021, according to Worldwide PC Forecast Update, 2021–2025: 2Q21, IDC #US48244121, September 2021), demand for computing solutions in the hybrid world is still outpacing supply. This requires organizations to creatively adapt, both by changing the way they think about remote access and by looking deep into their existing device pools to leverage existing assets.

Part of this rethinking involves using an old idea — applying lightweight operating systems with simple management requirements to low-cost or old equipment and then backing that with effective virtualization. This "thin client approach" has been part of the end-user computing story for decades, but it's only recently that the workforce has truly needed the solution.

What Changed?

During the initial stages of the pandemic, as office workers in particular went remote from their enterprise campuses to work from home, "remote work" drove an increase in the need for endpoints. Some endpoints were traditional laptops and desktops; others were purpose-built "light" devices such as Chromebooks or "thin clients" of various sorts. A cornucopia of solutions to support these devices and grant access to enterprise resources emerged, many of which relied on a combination of virtual private networks, virtualization, and the use of software-as-a-service (SaaS) applications for specific functions.

WHAT’S IMPORTANT

Hybrid work places unique demands on workers' workspaces and devices; meeting these demands will require new tools to allow end users to configure their own experience. Part of this rethinking will involve applying the lessons of the pandemic to use low-profile secured devices and extending the life cycle of existing devices by deploying dedicated lightweight, secured technology including cloud-delivered virtual applications and desktops.

KEY TAKEAWAYS

In the long term, hybrid work will force changes to the user and support experience as well as the device profile. These changes can be addressed through a balanced application of lightweight endpoints, traditional PCs, and a variety of virtualization options.
At the same time, corporations began a wholesale move of applications, data, and other workloads to public clouds. This created a condition where remote workers needed to access a mesh of resources located across a wide range of providers, using different security protocols, configuration options, identity management, and IT management consoles.

As the pandemic progressed, companies adapted to "hybrid work," augmenting remote work with collaboration, conferencing, automation, and mobility. Working remotely has shifted to working adaptively, both within and outside corporate locations and with variable schedules based on the shifting demands of geography, conflict, and daily life.

This highly complex environment exposes a variety of threat surfaces, including unmanaged devices and accidental data leakage from SaaS applications. This environment has inevitably led to an increase in security incidents, ranging from ransomware to state-sponsored infiltration of key management systems. These incidents have increased in both number and severity, with unprepared organizations finding themselves unable to work for days or weeks.

Part of the preparation to ensure security is the establishment of a model where the end user's workspace (data, applications, automations, context, etc.) and endpoint device are divorced from one another. The workspace (often hosted in a virtual computing environment using a combination of on-premises VDI and desktop as a service) can then be easily isolated if compromised and restored if necessary. The endpoint device can then be managed and secured using a zero trust model, reducing its relevance as an attack surface into the enterprise.

**Benefits**

This modern approach of splitting the workspace from the endpoint and using either old or lightweight devices brings with it a number of benefits.

**Customized User Experience**

Hybrid work's unique demands — from working asynchronously across teams to novel challenges with work definitions, locations, security, and access — require new ways of organizing and presenting digital resources. Technically, this requirement is met through a combination of collaboration and productivity tools, automatic and self-remediation of issues, application access through virtualization and other means, and user-designed automation including workflows and task applications. Practically, these technologies allow users to configure their own experience and then have that experience presented to them regardless of the device they use.

**Extended Time Frame for Refresh During a Time of Supply Constraint**

The shift to hybrid work, accompanied by a sharp increase in demand for additional devices, will not abate. In the long term, the supply of devices will come up to meet demand, but in the short term, organizations will have to adapt to getting the best, extended use out of the systems they can acquire.

This pressure to acquire will also lead to increased use of endpoint devices with lightweight operating systems and, potentially, less-than-optimal specifications, attempting to make up the performance and capability difference through the separation of workspaces and endpoint devices. Although this approach has historically been problematic, IDC expects that the unique pressures of the past two years and the next three years will lead technology providers to new, innovative solutions in this area.
**Lowered Operational Burden Due to Deployment of New Tools**

In IDC’s *Future Enterprise Resiliency and Spending Survey, Wave 11* (December 2021), 45% of companies indicated that providing IT support to hybrid users is a concern. This is due in part to difficulty in maintaining IT staff during the "Great Resignation" and in part to the dramatic uptick in support requirements caused by hybrid work. Using modern image and device management technologies allows the endpoint administration staff to meet the uptick in demand.

**Considerations**

As mentioned, the pandemic is not the first time that the IT industry has spun the story of using low-cost or older devices to support modern applications. It’s a well-worn canard, one that typically falls afoul of several challenges.

**Older Devices Require More Maintenance**

The electrical and mechanical elements of computing devices do wear out, at variable rates, especially when they are under electrical or mechanical stress. The older a device gets, the less predictable this pattern of wear becomes, leading to unpredictable maintenance requirements and odd behaviors.

**Systems Are Highly Dependent on Network Access**

Virtualized systems are, by their nature, highly dependent on reliable high-speed network access. Although the "5G revolution" has helped with this in some areas, large portions of the world’s workforce continue to work in areas where networks are unreliable at best. That these areas are also likely to have older, higher-maintenance client hardware just exacerbates the support issue.

**Additional Complexity Creates Increased Security Risk**

Although in theory purpose-built, security-conscious operating systems and workspace solutions are more secure, the reality is that the more moving parts a system has, the more attack vectors it presents. This can be mitigated by careful design and planning with a smaller number of strategic providers as well as constant security vigilance and careful application, but complexity cannot be ignored.

**Trends**

Chrome OS is one of several lightweight client approaches paired with both traditional VDI and desktop-as-a-service technologies like those provided by Citrix in the market that will be affected by the growth of hybrid work environments.

**Demand for Custom Adapted Workspaces Will Accelerate**

As hybrid workers begin to adapt to their new workloads, they will increasingly need to configure their digital workspaces into specialized forms. The general "one size fits all" approach adopted in the windowed format pioneered by Xerox in the 1970s will give way to more focused and adaptable computing, which uses a combination of natural language, integrated displays, and augmented/virtual reality to present information in context with the actions that need to be taken.
**Additional Support Burden to Accelerate into the Future**

The world of hybrid work, and its challenges, is an enduring change. This will increase and accelerate the complexity of support, creating additional need for both automation and threat surface reduction.

**Purpose-Built Security Comes of Age**

The current generation of solutions for the split workspace/device combination will continue to evolve, adapting to the new security concerns posed by increasing geopolitical conflict, hybrid workforces, and energy insecurity. This evolution will include the acceleration of artificial intelligence to address core configuration errors and simple attack vectors, along with refinements in the zero trust model for devices and expansions of the capabilities of cloud-provisioned workspaces.

**Conclusion**

In the short term, meeting the demands of hybrid work will force IT organizations to use their workspaces in new ways. In the long term, hybrid work will force changes to the user and support experience as well as the device profile. These changes can be addressed through a balanced application of lightweight endpoints, traditional PCs, and a variety of virtualization options including application and desktop as a service.

---

**About the Analyst**

**Shannon Kalvar, Research Manager, IT Service Management and Client Virtualization**

Shannon Kalvar is Research Manager for IDC’s IT Service Management and Client Virtualization Program, responsible for delivering research and advisory for IT executives, vendor management teams, and investment executives. Mr. Kalvar’s research coverage includes IT service management, desktop as a service (DaaS), virtual client computing, cost transparency tools, software asset management, and the use of AI and NLP for service management.
MESSAGE FROM THE SPONSOR

About Citrix & Chrome Enterprise

Citrix builds secure, hybrid work technologies that help organizations unlock human potential and deliver a consistent user experience wherever work needs to get done. With Citrix, employees get secure access to all of their apps and desktops, and IT has a unified platform to secure, manage, and monitor diverse technologies in complex cloud environments.

Citrix solutions on Chrome OS devices provide organizations with a cost-efficient and secure by design hybrid work solution to power a global, distributed workforce. Combined with Chrome Enterprise, Citrix and Google enable IT teams to centrally and remotely manage, define, and secure employee access to devices and any type of app or virtual desktop, all from the cloud.

To learn more about Citrix and Chrome OS, visit our website.