White Paper

Enable Workplace Transformation with Intelligent Digital Workspaces

Sponsored by: Lenovo

Phil Hochmuth
April 2023

IDC OPINION

The enterprise corporate workplace has undergone rapid and permanent change over the past several years, as widespread adoption of remote work and quick implementation of hybrid work structures have become the norm for most businesses. As the workplace undergoes this radical transformation, employees have also reimagined and reinvented their personal workspaces — the digital devices, apps, and tools workers use to do their daily jobs.

According to IDC's 2022 *Future of Work Survey,* all 1,316 respondents worldwide — 100% — said their organization has adopted, or plans to adopt, a hybrid work model. Among these firms, nearly half (46%) of enterprises worldwide describe their company's hybrid model as "flexible" or "very flexible" where employees can work freely between home and onsite offices.

However, big questions around how employees will interact, collaborate, and be productive in these new environments is still up in the air. While tools for remote collaboration have been available for decades, they've never been used at the scale seen in the past several years. Technology initially meant for a small subset of "remote" workers suddenly became the norm, a primary way employees interacted, shared information and, in general, worked together. Many such technologies in the market became synonymous with this new way of working. To that end, videoconferencing, cloud productivity suites, and content sharing and collaboration tools are areas of increased planned spend for more than 45% of enterprises worldwide and represent top 3 categories of technology investment, according to IDC's 2022 *Future of Work Survey.*

While many businesses accelerated the use of these technologies quickly and have come a long way in supporting hybrid, even now, more than half of organizations are still categorizing themselves, at best, as "moderately" ready for broad work transformation. Many organizations were forced to accelerate digital transformation efforts just to enable hybrid/remote workers but did so without a long-term sustaining strategy for supporting this environment for the long run.

With this new environment in place for most organizations, security has emerged as a top concern for IT professionals. In many cases, IT teams are being asked to open and unlock corporate resources, such as devices, internal apps and data, and other IT services, ahead of internal readiness for these technologies to be exposed and accessed remotely. Some firms have undergone rapid reimagining of their internal IT infrastructure and security architectures, while others have struggled to try and fit the new way of remote/hybrid work into existing, legacy infrastructures — with varying degrees of success.

One result of the expanded workspace environments of remote/hybrid users is the increased number of devices, device types, and operating systems (OSs) used in a worker's personal workspace environment. While Windows PCs are still the workhorse of enterprise digital work, more than 50% of enterprises say that other endpoint device types — ranging from Macs to Android and Apple smartphones and tablets are just as critical to end-user productivity and overall enterprise productivity. However, among these device types less than 50% (and in some cases more than two-thirds) of such devices are not managed by any corporate endpoint management software platform. This makes many end users' digital workspaces an open, broad multidevice/multi-OS attack surface.

According to IDC's December 2022 *Future Enterprise Resiliency and Spending (FERS) Survey, Wave 11,* the top 3 business priorities of enterprise CIOs are operational efficiency, customer satisfaction, and employee productivity (with more than a third of respondents citing these areas as top 3). Businesses have undergone a lot of change, pain, and revamping of infrastructure to reach these goals. However, the ability sustaining support for operational efficiency, enabling workers to delight customers, and driving more end-user productivity growth is a challenge that CIOs will continue to struggle with, unless there is a fundamental shift and rethinking in how IT can deliver and support such environments.

SITUATION OVERVIEW

The Intelligent Digital Workspace

An intelligent digital workspace (IDW) is an ecosystem of technologies that secures, personalizes, and interconnects the resources that employees need to be productive. This includes tools for collaborators, business software and apps, and critical databases and other data sources. IDW architectures allow for the access of all these IT resources from any location and on any device. IDW environments are also fully observable from an analytics and reporting perspective and provide IT teams with means to automate a wide range of end-user support, enablement, and security remediation tasks and workflows.

There are three fundamental product categories or "layers" to the intelligent digital workspace. While each layer of the IDW is in its own right a critical digital business tool for enterprises, it's the deployment of these three layers in concert, and in the context of the IDW frameworks, which differentiates businesses trying to play catch-up with digital and workforce transformation to organizations thriving as a result of a more agile, connected, and secure workforce.

Workspace Devices

Physical devices are a critical component to an individual employee's workspace, and the larger workplace in general. This layer includes devices such as PCs and laptops as well as smartphones and tablets and office-based peripherals (multifunction printers, desk phones, conferencing equipment, kiosks, point-of-sale devices, and ruggedized computing endpoints).

How devices are deployed relies heavily on use cases and industry scenarios (Windows PCs, Macs, and Linux desktop/laptops all have varying roles and levels of preference among employee types, ranging from knowledge workers, creatives, developers, and frontline staff). Ruggedized or low-cost Android tablets may suffice in back-office or transactional workspace roles, while for some firms with customer-facing retail or banking services scenarios, only the latest iPad will do. Physical devices and "things" in the digital workspace certainly go beyond PCs, desktop phones, laptops, smartphones, and tablets. Conferencing equipment, large-scale computing devices with touch interfaces, and smart

digital assistants will also be part of a connected, digital workspace — or "workspace IoT" — environment. Collectively, these individual technology deployment environments comprise the larger digital "workplace" environment. PCs, mobile devices, and collaboration/communication devices and endpoints are the primary components of these workplace environments today. In the near future (and already deployed among some forward-thinking businesses), augmented reality/virtual reality (AR/VR) and other connected, immersive wearable technologies will become integral part of enterprise workspaces and workplaces.

Devices are sometimes overlooked as commoditized technologies, but it is critical for businesses to ensure not only that workers have endpoints that are needed to do a specific job but that they also enjoy using their devices on a daily basis. Intelligent digital workspaces must accommodate all these options while extending security, management, and control capabilities across a diverse set of endpoints. According to IDC's 2023 *Endpoint Management Survey,* more than 90% of organizations now allow for some level of BYOD or personal device usage for work. End users are making choices as to what kinds of devices work best for them and putting the onus on IT and security teams to integrate these endpoints into a larger enterprise architecture. The IDW framework is a critical means to that end. This includes rebuilding access technologies for BYOD-centric users with technologies such as secure accesses service edge (SASE) and app-level VPN technology deployments.

At the same time, devices are proliferating in new use cases where endpoints such as smartphones and tablets or connected devices with embedded technology such as Android OS or IoT systems, such as Linux or Raspberry Pi, are acting as single-use or task-specific devices (such as tablets used to book conference rooms, or connected HVAC control systems, or digital signage/kiosks). Management and security of these deployment scenarios is as important as end-user computing management/security (if not more so) since deployment of these IoT workspace technologies can significantly increase an organization's digital attack surface and open up firms to escalating attack scenarios. Single-purpose devices, such as tablets or smartphones used as barcode scanners, or other data capture/input devices, can also be sources of data leaks and compliance violations, especially if such tools are used by multiple employees across work shifts and in multiple locations.

Workspace Apps and Experiences

Some workers might say they "live" in a certain application, software suite, or digital tool as part of their day-to-day job. This is where the digital experiences layer of the digital workspace operates. This layer unifies people, data, content, communities, and context to personalize and proactively surface the technological solutions that workers need to do their jobs. In recent years, line-of-business (LOB) leaders acquired these solutions to streamline their work, often circumventing existing processes in the name of productivity.

Collaboration and easy access to data and applications are key attributes of the digital experiences layer. Having this layer well integrated with the devices and infrastructure software layers allows digital experiences, data, apps, and other resources to be delivered to any device on any network or deployment scenario.

Deploying and integrating business applications, software, and SaaS resources through the IDW framework can remove barriers to employee speed and efficiency. In the IDW framework, software can generate proactive recommendations about the next best action and present the resources required to complete that action. This creates a consistent work environment in terms of data and app experiences, which can then be used to drive knowledge-powered solutions at the group, team, division level, or enterprisewide. As workers become more physically apart and their digital resources

increasingly more far-flung, tying together this level of digital engagement with IDW becomes even more critical. Along these lines, many enterprises are starting to address employee well-being and mental health with technology solutions. More than 40% of enterprise respondents in IDC's 2022 *Future of Work Survey* said they were implementing employee wellness programs with digital technologies over the next 18 months.

Workspace Infrastructure

This is the technology that ties together the device and apps/experiences layer of the IDW. Such platforms are the glue that keep together all aspects of the IDW into a unified experience. On a functional level, this includes tools that provide initial and ongoing provisioning, management, access control, security, monitoring, and support for hardware and software deployed in end-user environments.

Some software categories of these tools include endpoint device management, IT service management, virtual client computing, IT asset management, identity and access management, and endpoint security software technologies. AI- and ML-driven technologies such as advanced analytics, API management, and intra-app and platform connectors are also emerging in this category.

As vendors of digital workspace infrastructure consolidate, users will have broader visibility of data on end-user device configurations, compliance states, and software/apps inventories deployed in the enterprise. This is a big data source that, through AI, can be used to automate tasks such as software deployment and discovery, security monitoring of end users' systems, and other management tasks that are part of basic client endpoint management platform functionality. This automation can help users of the technology more efficiently manage and secure large fleets of devices across a wide range of form factors while supporting complex policies, rules, and configuration models. The ability to virtually deliver apps and even entire desktop experiences — often called workspaces in the industry — is another key capability in the digital workspace infrastructure layer.

Where the Layers Interact

Coordinating and organizing the three layers is an ongoing act of design focused on balancing productivity and behavioral enablement. Among a range of anticipated changes and challenges, enterprises worldwide cite this hybrid new work model as a factor that will permanently change their IT operations. As employees move toward hybrid work, intelligent digital workspace technologies will help bridge the gap between physical and digital environments as well.

Resource entitlement/assignment starts with onboarding, continues throughout the employee experience, and may well extend beyond formal completion of the work arrangement for an indefinite period. This entitlement must be dynamic instead of statically assigned to a specific position. These entitlements may include devices, interface configurations, and security arrangements/software within the infrastructure stack to enable critical process steps or behaviors. Examples include the suite of assignments, entitlements, and forms required to initiate employment; the management of information exposed in the interface based on geospatial and social (e.g., presence of teammates) location; and the management of retirement benefits after employment is complete.

With endpoint devices being such a critical component of the digital workspace, it's not a surprise that many enterprises would look to device OEMs as a top trusted partner for deploying critical workspace technologies, such as endpoint configuration, security, access management, and compliance. According to IDC's 2023 *Endpoint Management Survey,* more enterprise CIOs cited device

manufacturers/OEMs as their primary suppliers of unified endpoint management solutions (42%) compared with other technology supplier sources, such as software vendors, telcos or system integrators, and VARs. This strong connection between device supplier and the supporting workspace management and security technologies indicates that buyers of end-user computing technology see the role of device makers as not only going beyond just supporting hardware but also enabling the entire end-user computing experience, including security, management, and application provisioning.

This strong affinity toward endpoint devices and OEMs as key infrastructure partners makes sense. According to IDC's 2023 *Future Enterprise Resiliency and Spending Survey, Wave 11,* notebooks and PCs are still hot areas of investment and spending for enterprises. Worldwide, just under 50% of enterprises said they planned to increase spend on technology categories such as notebooks, smartphones, and tablets in 2023 compared with the previous year (even as a troubled economy and possible recession loom). This shows how much organizations rely on having a digitally enabled workforce and the strong association that businesses make between digital productivity and advanced endpoint devices.

System Infrastructure Focus: Unified Endpoint Management

Unified endpoint management (UEM) combines into a single software platform the management and provisioning functions for most common end-user computing operating systems and device types (e.g., Windows, macOS, iOS/iPadOS, Android, and Chrome OS, as well as Linux). By definition, UEM products must be able to manage both mobile and PC endpoints; this excludes legacy platforms such as PC life-cycle management, PC imaging solutions, and mobile device management.

Devices — laptops, PCs, smartphones, tablets, and wearables — are where the rubber meets the road for many enterprises' digital transformation projects. The introduction of new endpoint devices and device types into enterprise use cases and workflows requires centralized, or unified, management, monitoring, and configuration functions. This can ensure that endpoints are functionally optimized and properly configured, secured, and compliant from operating system as well as app and data standpoint.

Receiving a new corporate device — whether a PC, mobile device, or specialty endpoint — is often the first experience new employees have with an IT organization or the organization overall. Businesses have for a while tried to make onboarding experiences seamless and even consumer-like. This includes automated provisioning and updating of end-user environments, allowing new workers to start being productive immediately on the job. Organizations that are already oriented toward cloud-based system infrastructure, software, and business apps are in a better position to enable this type of scenario. However, organizations with strong UEM capabilities, especially cloud or hybrid deployment of the technology, will be in a better position to successfully take advantage of endpoint analytics.

Device as a Service — Enabling Intelligent Digital Workspace Infrastructure

Devices as a service (DaaS) combines hardware, on-device software, and life-cycle services into one as-a-service product with a consistent, recurring price. Users of DaaS generally see benefits in terms of cost savings as well as the ability to offload and shift IT department resources away from client endpoint device management, one of the more manual, labor-intensive resources roles in any IT group. Working with a DaaS provider integrates these functions into a company's broader IT operations without burdening or overextending human and technical resources. In addition, workers (the ones using the devices) also benefit from the DaaS model, as they receive devices that are more

suited for their role and task, as well as receiving shorter device upgrade cycles; so workers are always taking advantage of the latest technology and features from hardware OEMs.

There are some migration challenges associated with DaaS adoption. Many organizations might still have long-term service contracts on existing device fleets or are sourcing multiple device types from various sources (e.g., PCs from one provider, mobile devices from a cellular carrier). There is also a learning curve and ramp-up time for retraining and redistributing IT labor to other areas because of DaaS adoption. However, many organizations do see this as the future of the endpoint IT operations strategies. According to IDC's 2022 *Future of Enterprise Resiliency and Spending Survey,* 45% of enterprises said they saw "workspace as a service" offerings as being one of the enduring technology adoption areas that will last long beyond the COVID-19 and post-COVID-19 time frames.

Benefits of Intelligent Digital Workspaces

A characteristic of the modern work environment, or workspace, is the enormous amount of data generated by the interaction of devices, interfaces, and infrastructure. This data is a problem for some organizations because it forces context switching, which kills productivity. And it's a problem for the foundation of the agile workspace with its focus on detecting, contextualizing, organizing, and executing work as it occurs.

The primary differentiator of the intelligent digital workspace is intelligence. Intelligence is what personalizes the workspace for end users and provides the specific resources that a worker needs for the task at hand. An example of this may include an application deployment, dashboarding, or app launching aggregation tool, which knows the group, role, and digital needs of an individual worker and populates or provides only the necessary apps and tools automatically. Another example could be a workflow management technology that anticipates the next digital step or requirement for a worker in a given workflow or task and surfaces just the right app, piece of digital content, or access rights to the user seamlessly. This view of the intelligent digital workspace has not yet been fully realized, but innovative technology vendors and service providers are rapidly making progress, effectively turning the traditional means of technology delivery on its head.

Unlike work structures created in the mid-20th century, the intelligent digital workspace responds to work as it emerges from modern businesses' chaotic mix of data, people, processes, and partners, and it meets the demand for millisecond decision making. It creates a consistent context, maintains a flow of work, and organizes action by a combination of digital and human workers entitled to an array of data, digital, physical, intellectual, and workflow assets. While some organizations chose agility and were better able to navigate the disruptions of the COVID-19 pandemic, other firms suffered from compulsory, unplanned agility forced upon their workers and teams. Going into 2023, the majority of U.S. enterprises plan to increase spending on digital workspace technology to support new models of remote/hybrid work and address new demands and security challenges brought on by a distributed, dynamic, and borderless enterprise.

AI-enabled orchestration overlays onto the intelligent digital workspace. The worker is at the center of the intelligent digital workspace paradigm. Universal device access is the initial interface to a digital layer of applications, tasks, data, and work groups and communities. These interfaces, experiences, underlying data, and business IP are bound by the third layer — workspace infrastructure, which provisions and provides the guardrails, boundaries, and security tethers of the overall workspace based on business policies, compliance mandates, and other controls and requirements. AI, ML, and analytics technologies can proactively recommend the next best action and provide access to the resources required to complete that action.

From a pre-deployment scenario, analytics can be critical for helping suggest a better match of technology (endpoint devices), as well as key apps and software packages to employees based on their personas, roles, and skill sets. The deployment of AI and ML can also be used to proactively identify and self-heal issues on deployed endpoints before they turn into costly service desk issues.

CHALLENGES/OPPORTUNITIES

- **Incumbent tech:** Organizations have many tools and platforms to manage endpoint devices as well as to deliver software, provision environments, and create workspace experiences for end users. Many of these platforms are well entrenched and have a long tail in terms of their usage and legacy impact on an organization. Providers of IDW platforms should continue to offer capabilities to help customers support multiple types of environments and functions as organizations continue their migration to IDW frameworks.
- **Security turf lines:** The line between management and security of endpoint devices continues to blur and bend as functionality of modern devices more tightly integrates these functions. Keep security buyers, or multi-hat-wearing IT decision makers (i.e., teams managing both security and management products) in mind in terms of product messaging and demonstration of broader value.
- **Expanded digital footprint/attack surfaces:** As enterprises deploy more connected devices into employees' digital workspaces, and into the larger digital workplace overall, the risks grow for digital breaches, network intrusions, and other hacking-related activities. As more devices appear in employees' immediate digital workspaces – use of multiple PCs, mobile devices, tablets, connected endpoints, and so forth – there is more opportunity for hackers to infiltrate a business network by taking advantage of latent, undetected vulnerabilities inside device operating system software, or among applications and software programs running on devices. Also, the more physical devices become connected and "intelligent" in the digital workplace (e.g., IoT devices controlling HVAC, lighting, physical access) this also expands the attack surface for cybercriminals and digital bad actors.

How Lenovo Enables Digital Workplace Transformation

Lenovo's Digital Workplace Solutions (DWS) offering combines several digital workplace advisory services. Among these are persona-based endpoint device configuration and provisioning. This is a critical step in optimizing what types of devices, apps, and support functions are necessary based on business use cases and worker types. Collaboration and productivity tools and templated frameworks are also built out, as well as proper security software tools and services needed to support workers, their devices, digital activities, and goals.

There is also an integrated service desk function for ongoing support and incident management for end users. All these features adhere to the IDW three-layer model of workspace device, app, and support infrastructure framework and allow for end users to be as digitally productive as possible while getting technology into workers' hands more quickly and securely than in legacy deployment scenarios.

DWS combines several intelligent digital workspace technologies into a single as-a-service delivered solution, targeting organizations that want to transform their end-user computing environments without burdening existing IT staff and resources.

A critical component of this offering is the unified endpoint management platform, which underpins much of the delivery options from the technology. Lenovo's approach is to use market-leading UEM tools as the centerpiece of the solution. On top of these core platforms, Lenovo delivers multi-OS support for management, control, and security.

As enterprises adopt more types of endpoints, DWS can also expand to cover management and security use cases for endpoints such as augmented and virtual reality headsets (now being used in a wide range use cases across medical, logistics, field engineering, and other industries) as well as enterprise wearables for gathering and tracking critical business-related telemetry on employees' location and other activities, including environmental and physical safety.

Beyond the core capabilities of UEM, Lenovo offers a broader set of infrastructure software technologies that include encryption management for end-user devices, antimalware and antivirus technology for endpoint security, software license, and IT asset management tools as well as PC image management functionality.

This is a major differentiation. In Lenovo's DWS offering, compared with the way traditional PCs have been distributed and provisioned, device delivery times, as well as the time it takes users to go from device request to being productive working with a new device, are greatly reduced. Lenovo takes what was, on average, once a 10-step to 12-step process (involving long wait times for devices as well as manual and labor-intensive provisioning configuration and imaging of endpoints) and converts this into a 6-step rollout playbook.

With these features, Lenovo couples strong service-level agreements and ongoing measurements of end-user satisfaction and productivity with the technology tools it deploys. Using a combination of scoring techniques and data gathering (including D-Sat, Net Promoter Score, and Customer Support Effort) scores, Lenovo is able to continuously measure how workers are using the technology they've been given as well as measure the sentiment they have toward the technology itself. This delivers strong service satisfaction and keeps end-user productivity high.

In terms of intelligence infused into the offering, telemetry data is collected from managed endpoints constantly. This data is analyzed to monitor device performance, anticipate or predict potential failure of endpoint technologies, and detect anomalies in terms of endpoint behavior and atypical usage. These analytics capabilities built into the offering can trigger automated scripts to help quickly resolve discovered issues to minimize impacts to end-user productivity.

The end goal of DWS is not deployment and management of a certain IT product or service. It's to personalize end-user experiences, allowing workers to be collaborative and productive from anywhere, while leveraging organizational knowledge and expertise.

Lenovo helps deliver this with an omni-channel, single-touch point experience for DWS customers, allowing support and customer care to be delivered anywhere and at any time. This includes proactive, anticipatory support and IT problem resolution (i.e., seeing problems before they become trouble tickets and closing tickets quickly and efficiently if they do arise). This capability is fueled by Lenovo's robust cognitive AI, intelligence workflows, knowledge management, and personalization capabilities.

The vast breadth of Lenovo's offering in terms of geographical coverage is another advantage to the service offering. The capability is offered across 180 countries with major service hubs in North America, South America, Europe, and Asia.

CONCLUSION

Connected employees, partners, and customers are redesigning how work is done. Knowledge workers today are anyone, with or without a desk and company email address. They all create content and data that creates value for the enterprise. IDC has identified an increase in partners and end-user customers becoming part of an enterprise collaboration process. This is true for B2B and B2C companies. The consumerization of collaboration and other mobile technologies has created a collaboration-ready workforce. Partners and customers are slowly moving from the buyer-seller relationship to a maker-partner relationship where they are willing to help some businesses improve their offerings.

The move to hybrid work is reshaping traditional end-user computing management and security models. Tools must evolve to deliver enterprise-class services to remote teams. Convergence of roles, tools, and functions will disrupt traditional enterprise buying centers and channels. Organizations need to develop partnerships that will evolve with their needs.

Mobile, PC, and other endpoint management and activities are converging around a singular end-user computing management function. Any part of IT that touches the end user (devices, security and management/support tools, and apps) should incorporate the concepts of the intelligent digital workspace.

Device management and endpoint security are becoming increasingly intertwined and integrated. In summary, enterprises looking to digitally transform their workplaces and workspaces will be in the best position to succeed if they can align IT organizational functions, roles, and tools using services such as Lenovo's DSW offering.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com