SPOTLIGHT
Sponsored by: DXC

Any part of IT that touches the end user (devices, system infrastructure software, and apps) should incorporate the concepts of the intelligent digital workspace.

Enabling a Resilient Workforce with Intelligent Digital Workspaces

December 2022

Written by: Phil Hochmuth, Program Vice President, Endpoint Management and Enterprise Mobility

AT A GLANCE

KEY TAKEAWAYS

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, system infrastructure software, and apps) should incorporate the concepts of the intelligent digital workspace.

Introduction: New Challenges to End-User Computing Environments

With the adoption of more hybrid and remote work policies, employees are testing corporate boundaries and policies by redefining the corporate workspace, from the physical location to the devices, apps, and tools they use to do their jobs. They are also depending on employers to provide secure access to the data, applications, and colleagues that are essential for getting their work done.

Many organizations were forced to accelerate digital transformation efforts just to enable workers in these new environments. This involved intensifying their focus on securing both devices and data to the clouds and networks that support them while also maintaining privacy and compliance controls.

As increasingly distributed and hybrid teams come to define modern ways of working, security will remain a primary priority. It is an essential prerequisite to enabling employees to access the key resources they need — and yet the challenge ahead is to embed security measures as much as possible while moving away from today's friction-filled user experiences.

The global lockdowns early in the pandemic exposed existing security issues around supporting remote work at scale. These issues included the need to accelerate migration to the cloud for organizations that had delayed doing so, VPN access, and access to essential devices and hardware in the face of supply chain disruption. People sent home without laptops or mobile devices picked up what was available from outside retailers and logged into productivity, communications, and collaboration platforms — some that were approved/managed by IT, and others that were not. IT organizations are familiar with the cat-and-mouse game of assessing, managing, and allowing/denying the type of personal/consumer computing technology that workers are using.

Nonetheless, from a device standpoint, teams have had to deal with a large influx and infusion of bring-your-own-device (BYOD) smartphones and PCs coming online and accessing corporate data and apps. From a PC perspective, this has led to more diversity of device types. For example, sales of Apple Mac PCs surged in 2020. U.S. IT organizations say that as much as 23% of their PC fleet is now represented by this traditionally noncorporate desktop OS, which many Microsoft-centric support organizations are not trained or equipped to handle.

Behavioral enablement is sometimes mistaken for productivity enhancement because both focus first on minimizing context switching and then gathering required digital and physical resources to achieve an end. But productivity focuses on the creation of a specified output (e.g., a report, a process document, or a manufactured good), while behavioral enablement focuses on organizing information into patterns and connecting people with similar interests to work toward successful outcomes.

Expanding Access, Attack Surface, and Risk

The approaches to defending devices and data in this new paradigm have introduced other risks for IT. Many firms have had to extend VPNs into workers' homes to ensure secure computing activity. This blending of environments itself introduces new risks. Unmanaged or unknown endpoint devices and insecure home Wi-Fi networks can affect both corporate IT and the organization's security posture.

IT teams have also had to apply principles that were once relevant only to a specific segment of the mobile workforce — frequently traveling employees, or "road warriors" — to a much broader swath of the worker population. IT security teams now must account for lost/stolen devices at a greater scale as well as more frequent network access and activity from multiple locations. While risks such as airport or public space Wi-Fi may diminish, home Wi-Fi or even adjacent neighborhood networks have become a larger part of the threat model. Historically, IT could easily manage the occasional employee request for access to data, files, and computing resources from an asset left at home while working in the office (or vice versa). Given the shift in working patterns, IT teams need new approaches and thinking about how to scale these types of requests in massively hybrid organizations.

Returning to office environments, either full time or part time in a hybrid scenario, requires tight coordination between IT security and the teams that handle physical security, office management, and building operations. Management of facilities to ensure a safe return to work includes a wide range of considerations and responsibilities, such as ensuring surfaces and common areas are regularly cleaned and disinfected. Teams must also consider physical distancing and new space/layout requirements for offices and desks as well as use of shared resources. This planning and implementation activity intersects with IT and information security in several areas. Less obvious but also important are the security requirements for Internet of Things (IoT) devices or those fixtures enabled with IoT capabilities that have potential to expose network vulnerabilities.

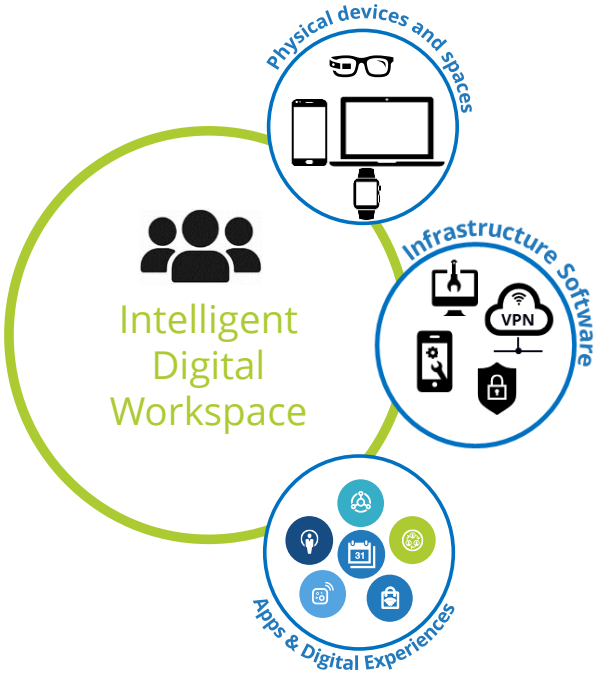
As if these challenges were not enough, they have been paired in turn with network integrity issues, an increase in cyberattacks (especially phishing), and the potentially negative impact of these factors on brand integrity. Customer and employee data privacy has been and continues to be a key concern as customer-facing workers and HR professionals work from home (WFH). Data and infrastructure security has also been a key part of the security equation. For example, users are increasingly blending personal and corporate cloud storage, email, and collaboration platforms to make WFH work properly. Remote and hybrid users may use noncompliant cloud storage or sharing technologies while trying to get their day-to-day work done. And while employees with personal devices or storage accounts may trust these consumer services, enterprise IT will have specific policies that restrict usage of nonauthorized content sharing or storage applications.

The Intelligent Digital Workspace

IDC defines the intelligent digital workspace as an ecosystem that offers an integrated user experience augmented by cognitive technologies such as artificial intelligence (AI), machine learning (ML), and advanced analytics. It provides a secure, personalized, and federated view of the resources that workers require to get their jobs done, including collaborators, applications, and data, from anywhere via any device. The intelligent digital workspace is also fully observable and optimizable by IT and security operations professionals.

IDC defines intelligent digital workspaces as consisting of three distinct layers of technology: physical devices and spaces, digital workspace infrastructure and applications, and digital experiences (see Figure 1).

FIGURE 1: ***Layers of the Intelligent Digital Workspace***



Source: IDC, 2022

The interaction of the three layers (device, interface, and infrastructure) enables the intelligent, agile workspace and the key behaviors that enterprises need to achieve business outcomes. In the current environment, this is most obvious in areas such as behavioral enablement, collaboration, resource entitlement to flexible roles, onboarding/offboarding, and the hybrid physical/digital workplace.

Physical Devices and Spaces

The physical devices and spaces layer is how workers interface with the intelligent digital workspace. It includes traditional devices such as PCs, workstations, and laptops (and all associated hardware) as well as mobile endpoints (smartphones and tablets) and other office-based peripherals (hardcopy multifunction printers, desk phones, conferencing equipment, kiosks, point-of-sale devices, and ruggedized computing endpoints). While becoming somewhat commoditized over the years, endpoint computing devices are still a critical interface layer for employees.

The forces of consumerization, as mentioned previously, shape a wide range of preferences (Windows or Mac), form factors (PC or smartphone), and even ownership and adoption models (company owned or BYOD). Intelligent digital workspaces must accommodate all these options while extending security, management, and control capabilities across a diverse set of endpoints. The saying that "the glass still matters" takes on new relevance in a diverse enterprise endpoint computing environment where preferences and bias can be strong and as many as six operating systems must now be accounted for (i.e., iOS, Android, Windows, macOS, ChromeOS, and Linux). What devices are deployed relies heavily on use cases and industry scenarios. (Windows PCs may be fine for most, but not for creatives or software developers. 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.

Digital Workspace Infrastructure

Underlying the physical devices and software layers of the digital workspace are workspace infrastructure platforms. Such platforms tie these solutions together and provide initial and ongoing provisioning, management, access control, security, monitoring, and support for hardware and software deployed in end-user environments. From an IDC software taxonomy perspective, these components include unified endpoint 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.

While each of these technology areas is a distinct market and domain, IT suppliers are shifting from providing complex suites of products to creating curated platforms that provide an integrated body of services in support of a business solution. This shift is further informed by the evolving notion of a "digital workspace," a productivity environment in which IT resources (including applications, analytics, productivity, and reporting) are integrated together on a managed or unmanaged platform.

As management, security, asset tracking, and support around endpoint devices consolidate, vendors 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.

Digital Experiences and Apps

The digital workspace is the modern-day control panel (or interface) for the flow of work, customized at the individual worker level. It 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 leaders acquired these solutions to streamline their work, often circumventing existing processes in the name of productivity.

Designed for collaboration and easy access to the data, content, and corporate IT systems, intelligent digital workspaces cross internal silos, are fully functional across all devices, and support corporate privacy, compliance, and governance requirements. Their core function is to combine the flow of work (and not just workflow), conversation, and communication layers within a secure platform that enables integrated, easy access to other IT stack investments customized for each worker.

Adoption of intelligent digital workspace technology can help remove barriers that slow down work, generate proactive recommendations about the next best action, and surface access to the resources required to complete that action. Such technology also creates a consistent supply of clean data and content, which can then be used to drive knowledge-powered solutions at the individual, team, and enterprise levels. When paired with a culture of collaboration, the intelligent digital workspace becomes the basis for enterprise knowledge management. Given the disruption of the traditional physical workplace caused by COVID-19, enterprises worldwide plan to increase investments in a range of technologies spanning the three layers of the intelligent digital workspace with the goal of improving employee productivity, collaboration, and satisfaction.

Where the Layers Interact

The hybrid digital/physical/social workspace is the most obvious intersection of the three layers of the intelligent digital workspace. Coordinating and organizing the three layers are ongoing acts of design focused on balancing productivity and behavioral enablement. Among a range of anticipated change 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. It 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.

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. 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 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 proactively recommend the next best action and provide access to the resources required to complete that action.

Considering DXC Technology

DXC Technology helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private, and hybrid clouds. Some of the world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. DXC, in partnership with Microsoft, offers the next generation of enterprise and workforce modernization and security for modern device management. This set of innovative solutions is designed for both the individual user and the enterprise through a combination of familiar and progressive technologies including multicloud, business apps, artificial intelligence, and mixed reality.

DXC's approach enables employees to work, connect, and collaborate from anywhere — seamlessly and securely — without disruption.

At the heart of this strategy is a set of persona-based technology and support services that aspire to enhance employee productivity and satisfaction. The key components include:

- Promoting employee productivity via a centralized management platform that anticipates and intelligently delivers support services when and where needed
- Onboarding new employees quickly and securely with persona-based devices, applications, and technology solutions that enable employee satisfaction and productivity
- Delivering security that improves both cyber-resilience and employee experience through DXC's portfolio of digital identity capabilities
- Measuring qualitative and quantitative service metrics continuously to understand and evolve technology efficacy, performance, and experience

Taken in concert, these principles drive top-level outcomes for the future of work scenarios accelerated by the pandemic and digital transformation objectives.

Centralized Management

At the core of DXC's efforts to deliver on the vision of intelligent workspaces is DXC UPtime, the company's experience platform. UPtime enables an organization to consolidate its workplace services and intelligently simplify the management of its IT assets, tools, and employee service delivery. Benefits for employees include robust automation and self-service capabilities. Benefits for the employer include a unified employee experience along with consolidation of rich experience and operational data.

According to DXC, its customers have seen improved employee satisfaction scores as a result of the ability to get rapid responses via interactions with the intelligent digital assistant and instant message chat when working remotely. Employees can raise new service requests or get their questions answered more efficiently to drive their productivity without waiting for help to diagnose technology issues.

Rapid Service Onboarding and Fulfillment

DXC collaborates with an organization to first identify and define the persona-based device, application, and security profiles that provide employees with the capabilities they need to effectively conduct their work using Microsoft Intune, Azure Active Directory, SCCM, and Active Directory Services. Using these standard persona definitions, DXC employs automated fulfillment and delivery capabilities that enable employees to quickly obtain requested services. Employee persona and service capabilities are routinely reviewed for refresh as the organization evolves and role dimensions adapt to changing demands.

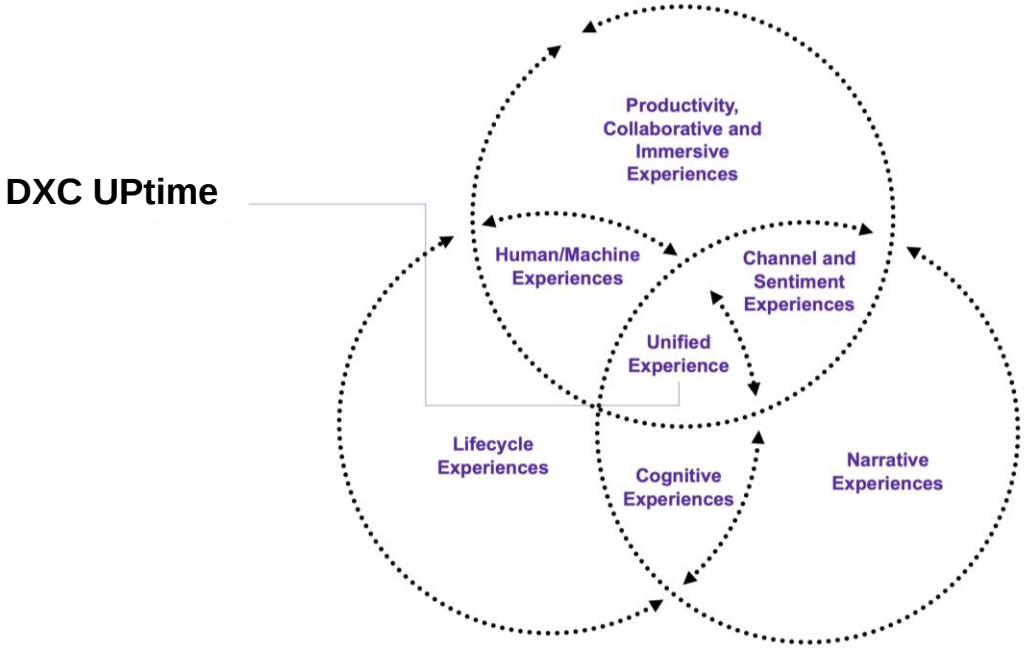
According to a case study provided by DXC, it assisted a multinational food and beverage company in quickly onboarding users from a recently acquired start-up firm. The effort required DXC to support the remote enrollment of each user into new security personas that were compatible with internal audit controls and to avoid financial penalties and liabilities. The program required execution in approximately 60 days and concluded with accurate hardware and software asset inventories to support asset purchases and license compliances. As a result of successfully completing this effort, the company was able to integrate the new users into its broader corporate ecosystem while avoiding negative audit findings and financial impacts.

Unifying the Employee Experience

Delivery of impactful intelligent workspace experiences requires continual measurement and refinement to remain effective. DXC has formed a strategy to unify all experiences across its portfolio and present them to the market as a set of interconnected and complementary experiences.

DXC employs a rigorous employee experience management (XM) framework that establishes a hierarchy of experience domains, from customer experience (CX) to employee experience (EX) and user experience (UX), each with its own quantifiable metrics for success (see Figure 2).

FIGURE 2: ***Modern Workplace Portfolio Experiences***



Source: DXC, 2022

Underpinned by a data-driven feedback loop and dedicated XM improvement team, DXC uses an agile and iterative approach to bring service and product improvements via advanced analytics capable of reporting user sentiment, workforce perception, and operational metrics. The experience improvement cycle complements existing CSI frameworks; however, the addition of a real-time feedback loop helps accelerate change that drives operational benefits, adoption, and increased ROI.

DXC teams analyze and detect problems, and they also drive actions to integrate and subsequently automate solutions to improve employee and end-user experience via the following:

- Quantitative and qualitative insight gathering to synthesize business processes, objectives, and employee use case requirements, utilizing the framework to track and measure overall benefits and value
- Current state analysis, user research, and employee persona creation, modification, or validation
- Continuous sentiment management with iterative capture and analysis to pinpoint priority areas that enhance technology experiences to drive ongoing improvement and innovation

Built with Security in Mind

DXC seeks to enable organizations to be cyber resilient through end-to-end security solutions that support digital transformation.

This includes an integrated portfolio of capabilities in collaboration with its extensive network of partners, comprising the following:

- Secured infrastructure to protect applications, infrastructure, and endpoints from exploitation
- Cyberdefense to address security breaches by quickly detecting and rapidly responding to threats
- Digital identity enabling people and machines to securely access data and services
- Security and risk management to enable full visibility of people, processes, and technology security risks to help the organization make better business decisions

DXC can deliver integrated capabilities across all these areas to create a true zero trust environment.

Challenges

The long tail of traditional client endpoint management will require many organizations to continue to use a mix of tools to manage their intelligent digital workspaces. Providers of unified endpoint management (UEM) platforms such as DXC should continue to offer capabilities to help customers support both types of endpoint management functions as organizations continue their migration to UEM and modern device management.

Enterprise IT decision makers see the single-pane-of-glass benefit of UEM as its greatest feature. Providers of UEM products such as DXC should continue to combine capabilities for device monitoring, management, and reporting across all major endpoint OSs (Windows, macOS, iOS/iPadOS, and Android).

The line between management and security of endpoint devices continues to blur and bend. DXC and other providers need to keep this in mind in their product messaging and demonstrations of broader value, which should speak to security buyers and IT decision makers overseeing security and management products.

Conclusion

Connected employees, partners, and customers are redesigning how work is done. They all create content and data that generates 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 consumerization of collaboration and other mobile technologies has created a collaboration-ready workforce.

The recent transition to more remote and 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, system infrastructure software, and apps) should incorporate the concepts of the intelligent digital workspace.

Device management and endpoint security are becoming increasingly intertwined and integrated. Enterprises must align organizational functions and tools to be more integrated across management and security domains. Rather than force fit management or security technology into device use cases and workloads better served by other tools, enterprises should deploy management and security in the context of the digital workspace and the type of work being done.

About the Analyst

Phil Hochmuth, *Program Vice President, Endpoint Management and Enterprise Mobility*

Phil Hochmuth is the Program Vice President on IDC's Enterprise Mobility team. His research provides insights into how enterprises deploy mobile devices and applications as well as management and security platforms. Key markets he covers include enterprise mobility management (EMM) and enterprise mobile security, including mobile data and threat protection and mobile device security technologies.

MESSAGE FROM THE SPONSOR

Global strategic partners for over 30 years, DXC and Microsoft modernize solutions across industries to connect people, data, and processes with tangible business results. We do this working with customers wherever they are on their transformation journey by providing professional and managed services across cloud, workplace, applications, security, and analytics. If you are looking for an independent scope and solutions to complex problems, consider DXC to be your technology partner. Reach out to us here.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.