Lenovo Unified Workspace

Technical White Paper

How you can deliver a web-based workspace for the modern workforce.

Overview

Lenovo Unified Workspace is designed to address a common IT problem: how to make apps and data readily available on unmanaged and remote devices without compromising network security, increasing costs or adding complexity.

With two-tiered security to keep users at bay, Unified Workspace enables IT to provide consistent user interactions with company data—without ever connecting remote users directly to the organization's datacenter. Companies can securely provide access from anywhere, at any time, through a single interface that delivers a consistent user experience across devices and operating systems.

In this white paper, we provide an in-depth look at the technical aspects of how Unified Workspace:

- Uses a two-tier architecture to keep private IT applications in the datacenter while providing remote access
- Leverages existing authentication requirements for single sign-on
- Unifies access to public cloud services and legacy storage
- Differs from other solutions such as hosted desktops and VPNs
- Can be deployed quickly with minimal on-premise requirements for many organizations

TABLE OF CONTENTS

INTRODUCTION

Today's work practices are rapidly evolving. As recently as a decade ago, the majority of devices used by employees were still desktop and laptop computers selected, owned and managed by IT. Work was done on these work computers; personal tasks were executed on separate home PCs. Today's average employee, by comparison, is in possession of three or more* devices—a mix that includes smartphone and tablet—and continually moves back and forth between them throughout the course of a typical day. As daily dependence on these personal devices grows, so does the expectation to rely on them for work purposes.

As a result, the demands on IT have shifted. Once the solid ground upon which every office and workspace was built, IT teams are now being tasked with extending data and documents far beyond company walls—not to mention beyond company-owned hard drives and networks. This presents a number of obstacles. How can IT make apps and data readily available on a wide variety of devices and operating systems? What steps must be taken to ensure a consistent user experience? How does a company maximize security when so many devices lack IT oversight?

Lenovo Unified Workspace is designed specifically to answer these questions and others like them. This workspace aggregation solution allows IT to deliver a single, secure, web-based portal that gives employees single sign-on access to all the apps and data they need, from any device and on any network.

*Source: globalwebindex

VPN AND VDI LIMITATIONS

For years, many companies have relied on VPNs, hosted desktops or both when extending user access.

Virtual Private Network (VPN) Challenges

VPNs are a popular choice because they enable employees to access local area network resources remotely through encrypted public network communications. But while VPNs help solve some of the biggest security risks when transmitting data over the internet, they can create a new set of obstacles.

- Commonly used on Windows desktops and laptops, implementing VPNs on smartphones and tablets—not to mention iOS, Android and Linux—can be incredibly complex
- The need for individual PC client installs, which often presents difficulties for non tech-savvy, offsite users
- VPN access is limited to the system on which it's installed, which in turn restricts the total number of devices that have access as well as flexibility for offsite connections to applications and files
- The level of user involvement with VPNs often necessitates ongoing IT maintenance and help desk requests for basic tasks
- VPN connections grant offsite access to onsite internal resources, which—despite firewalls—can be exposed if the user endpoint is compromised

Hosted Desktops Challenges

Because Virtual Desktop Infrastructure (VDI) provides access to personalized desktops powered by operating systems and application software inside a virtual machine, there's reduced need for endpoint hardware upgrades and updates. However, there are other challenges for IT.

- Server storage consumption increases with the number of users who require different sets of apps and settings
- The costs of required server hardware, storage and network equipment can exceed those of providing and maintaining individual PCs
- The hosted desktops that are reliable with a keyboard and mouse can be unreliable on mobile touchscreens

Overarching Problems for IT

The challenges associated with solutions like VPNs and hosted desktops often strains IT-employee relationships. An inconsistent user experience and frequent technical barriers to productivity for employees can lead to decreased adoption rates and increased training and support needs. In addition, dissatisfied employees may create their own unsecure workarounds or engage in risky behaviors such as browser password storage and unauthorized cloud storage, thereby exposing the company to heightened security risks.

The bottom line is that, for the growing business especially, keeping employees happy and data safe requires a truly cohesive workspace aggregator that maximizes the employee experience and minimizes IT maintenance.

WHAT IS UNIFIED WORKSPACE?

Lenovo Unified Workspace is designed to leverage existing directory services and current IT infrastructure for a secured, unified work area that provides the same environment across multiple operating systems. It can be used to create a simple, device-agnostic experience that connects end users to the apps and data they need—public and private web-based applications, legacy Windows apps, remote desktops, file shares and so on—at any time, from anywhere, and with minimal maintenance on the part of IT. Built on HTML5 web technologies to run inside a variety of browsers including Chrome, Firefox and Safari, the interface dynamically adapts to the type of device currently in use for a seamless experience. In less than three days, Unified Workspace can be deployed and integrated seamlessly with existing infrastructure to:

- Provide single sign-on (SSO) access to all files and applications, without the need for VPN and additional firewall rules
- Maintain a security protocol of thick layers including authentication, SSL, role-based access and other measures that isolate users from the company's datacenter
- Allow employees to more easily interact with all their apps and data from one centralized point of access
- Enable employees to self-enroll, self-provision and navigate through their day-to-day IT needs with a high level of self-sufficiency

Rather than simply opening the doors that separate different digital environments, Unified Workspace aggregates them into one cohesive work area that's mirrored across devices and networks, dramatically simplifying IT management.

The HTML5 framework supports all modern browsers including Internet Explorer, Chrome, Firefox, Edge and Safari, and the dynamic interface adapts to the type of device being used. Users only see the tiles that are relevant to them, based on IT-assigned permissions.

With more companies embracing agile work environments, web-based digital workspaces provide a variety of advantages. These range from cost savings derived from secure bring your own device (BYOD) policies to one lean IT infrastructure capable of supporting users distributed across hundreds of physical office locations. And as occasional telecommuting gives way to full-blown remote workforces and flexible plans that allow people to work where and when they're most productive—be it a cubicle during work hours or the living room couch at night—the need for portability of business property has risen sharply in a short amount of time. Unified Workspace brings order to the chaos so that IT can:

- Deliver IT services through the web
- Allow secure remote access to apps and data on personal devices
- Give users access to public and private resources with a single password
- Enable BYOD policies that don't create significant security risks

HOW DOES UNIFIED WORKSPACE WORK?

Unified Workspace addresses several critical components of anytime, anywhere connectivity.

1. Secure Architecture

Unified Workspace employs a two-tier architecture that keeps private IT applications in the datacenter while still providing access to remote users. This technology terminates users in the DMZ while still providing secure access to private datacenter resources through a single, secure port.

User access starts with Unified Workspace webRelay, a server in the DMZ that acts as a secure entry point to provide SSL and isolate remote users. The DMZ sits behind a WAF, which includes an IPs and IDs. The solution has been engineered to support existing directory service credentials for authenticating entry, allowing IT to leverage existing users, groups and organizational units. Initial login is secured by a variety of two factor authentication methods including image challenge, CAPTCHA, RADIUS tokens and one-time password providers (OTP).

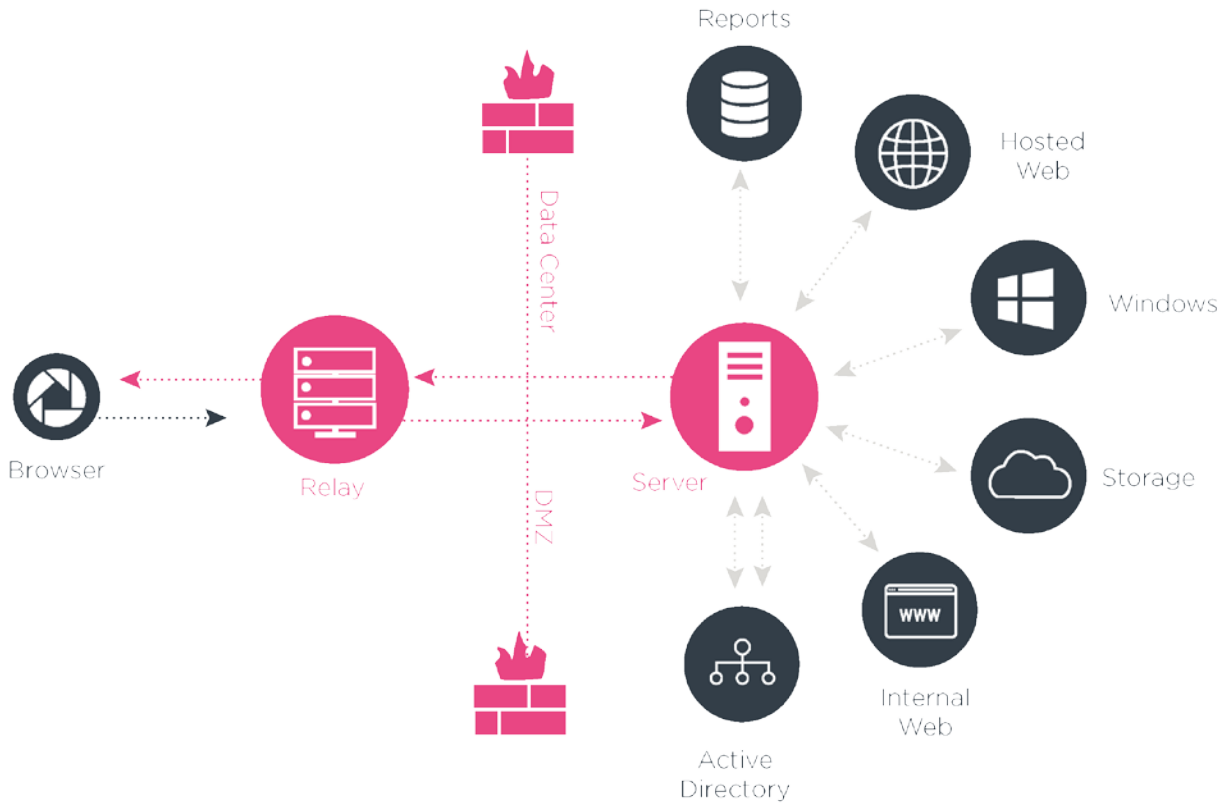
Once access has been authenticated, users are isolated inside the DMZ where physical access to the internal network is prevented. All traffic between devices and the Unified Workspace are encrypted. Many users may think they're connecting directly to assigned internal resources or protected enterprise SaaS apps—when in fact the relay is acting as a reverse proxy to provide access without the user actually joining the network.

Users see only what IT has decided they have access to, which is assigned using the company's existing LDAP directory groups and OUs. For organizations with heightened security needs, an optional secure browser can be used to force compliance on unmanaged devices and prevent unauthorized data removal. Any time you determine an application or site requires a higher level of security, IT can configure the session so that a user will be directed away from default browsers and into the Quarri Data Safe™ secure browser. This secure browser has extensive malware defense features that block hidden keyloggers, screen capturers, session hijackers, and other advanced malware from accessing or affecting the protected content.

The on-premises footprint for supporting this two-tiered architecture is small. The minimum requirement, which will suffice for most organizations of up to 4,000 users, is two servers: one internal Unified Workspace server and one dedicated, public-facing DMZ relay. The solution is platform-independent and can run on most current server operating systems, as long as they meet basic criteria:

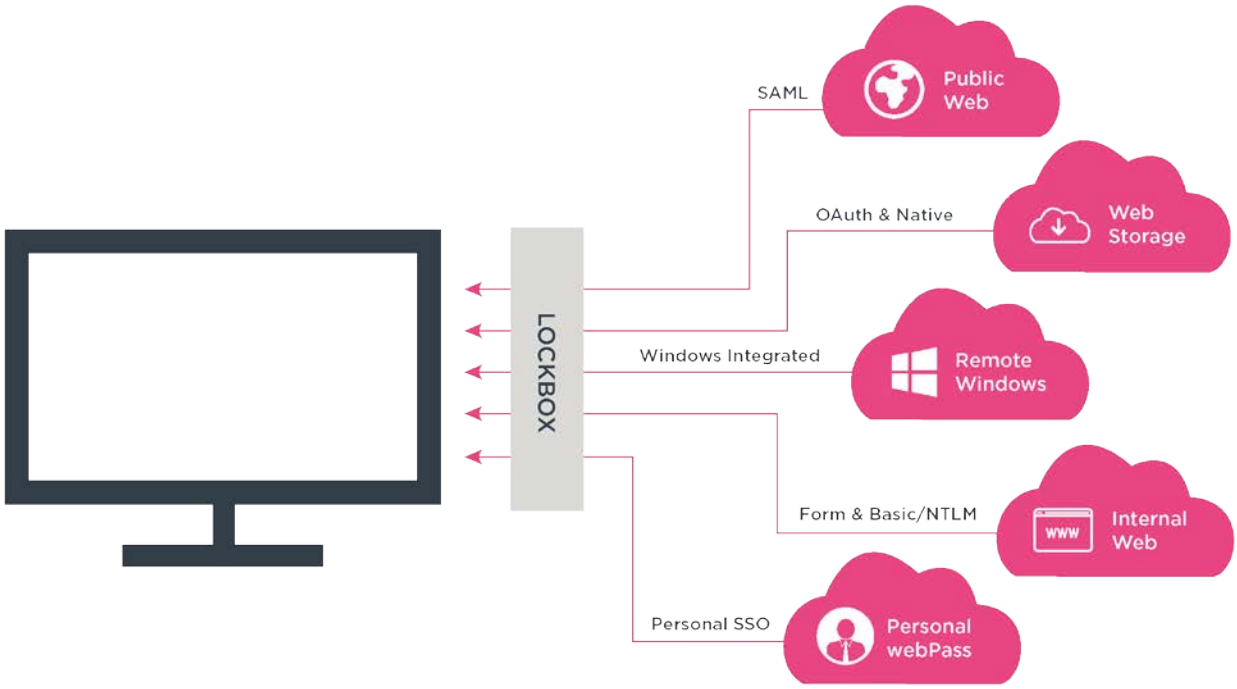
- 64-bit, four-core processor, 2.5 GHz minimum per core
- 16 GB RAM
- 20 GB hard disk partition
- 64-bit OS

That's it. There are no workstation clients to install or system requirements to worry about.



2. Access

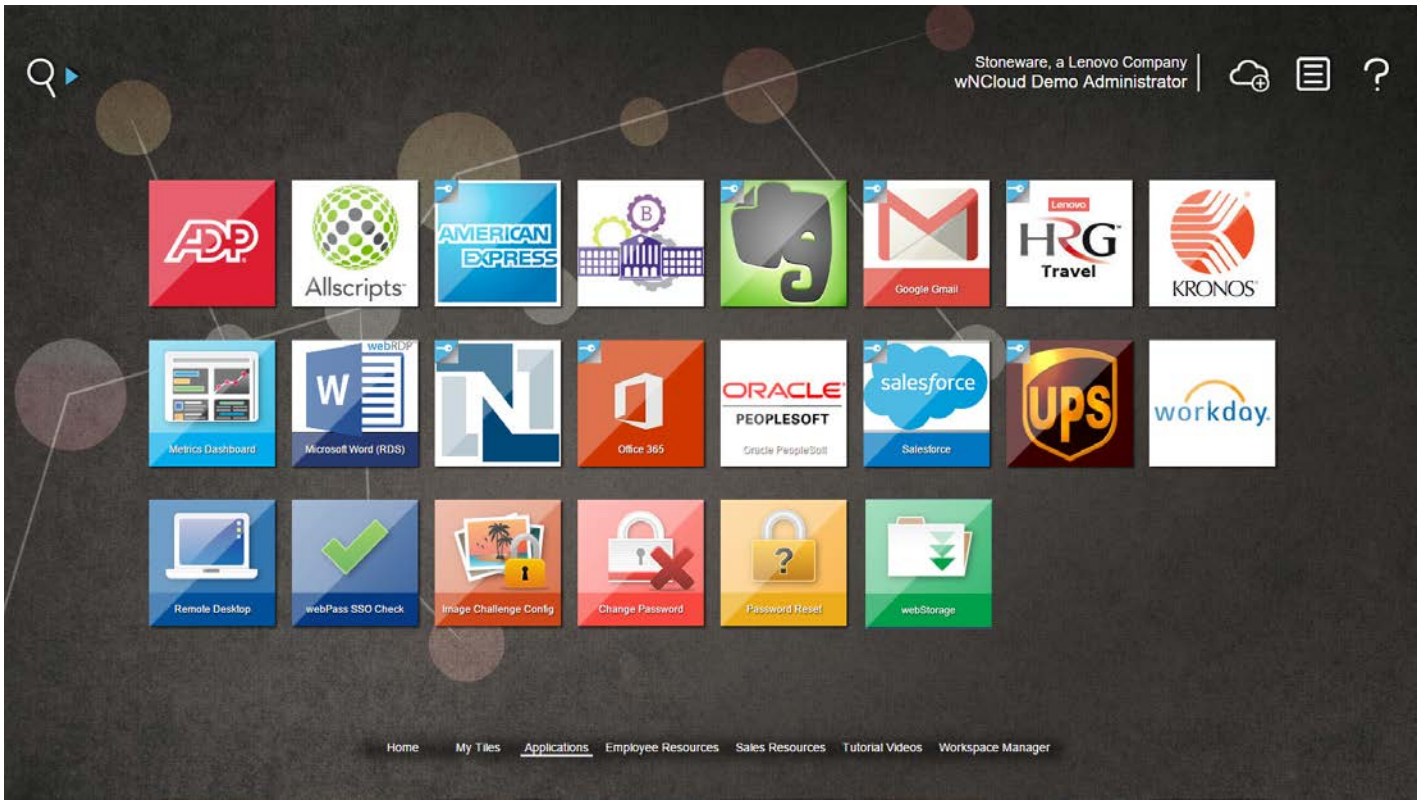
The web-based structure of Unified Workspace allows IT to provide one-stop access to apps and data through a central "hub" of activity that isn't reliant on device endpoints and user input. This structure allows IT to essentially forget about whether or not users have the right system requirements and software installed. Employees are granted access through a single user ID and password that can be used on any device without compromising the network. Enabling single sign-on allows users easy and secure access to their applications all from one central starting point.



Once a user is authenticated to the organization's Unified Workspace, the server can pass credentials directly to other apps and resources so that person won't have to manually log in to each resource. Unified Workspace can leverage existing authentication requirements by using industry standards like SAML, ADFS, and NTLM. An existing directory service—Microsoft Active Directory, Novell eDirectory and OpenLDAP are all supported—is used to validate logins and provide role-based access.

For other applications that are not configured to interact with the directory or leverage a standard like SAML, Unified Workspace offers a form-based authentication system called webPass. The first time a user wants to access one of these apps, he or she is prompted to enter an existing username and password. The information is secured using strong AES 256-bit encryption and stored centrally so that future logins happen automatically—whether from the same device or a different one.

From the user perspective, this setup allows employees to select the apps that work best for them and have instant access to everything in one place through click-and-go tiles. They simply type in the organization's Unified Workspace URL and click away. Again, there's no software to install and very little, if any, training involved. The onboarding process can be done in a day.

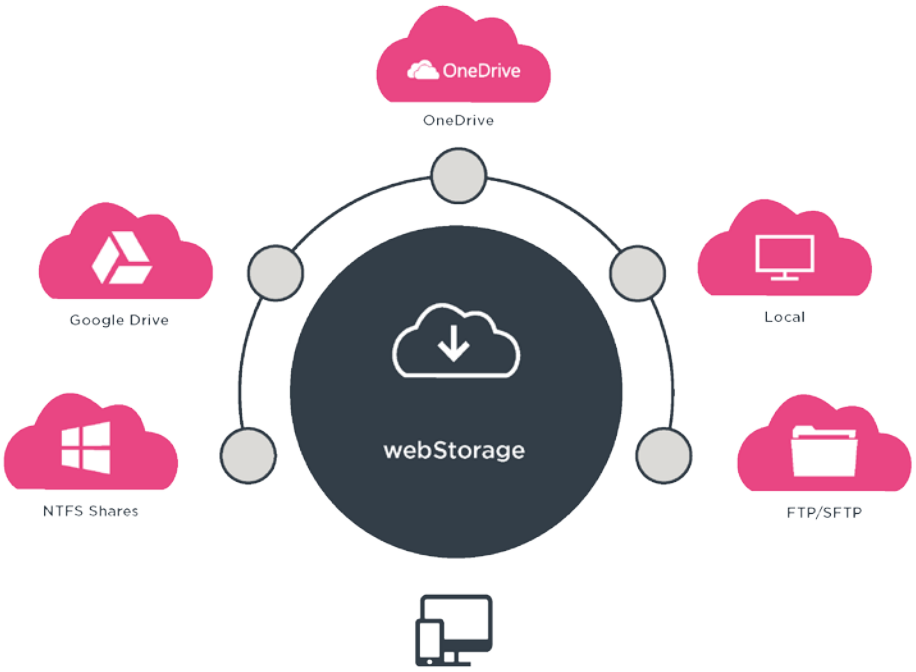


Users can access the Unified Workspace interface through any modern browser with JavaScript and HTML5 support.

3. Delivery

Many businesses have found an answer to faster file sharing in cloud storage services, which can free up precious space while making it easier to access and share documents on the go. But since work environments are still at the intersection of old and new, many organizations struggle to merge these public cloud services with legacy storage.

The Unified Workspace webStorage component unifies public and private storage into one central interface where FTP, SFTP or CIFS shares meet cloud accounts. With minimal effort on the part of IT, Unified Workspace can be used to provide users with a unified view of files stored in the public cloud or on internal network shares and home directories from any location—and allow modifications without the need for a VPN. The HTML5 interface and web-based file explorer allows centralized access to internal files as well as cloud storage services such as Box, Dropbox, Google Drive and OneDrive.



From here, IT has three options:

1) Allow employees to download files and use local applications to edit and reupload them

2) Enable files stored on OneDrive or Google Drive to open directly in corresponding cloud-based editing tools such as Office Online and Google Docs

3) Connect users to a published remote desktop powered with Live Edit functionality, eliminating the need to download files to local devices

One, two or all three options may be implemented, allowing IT to provide a range of editing options—from Office Online to the full Microsoft Office suite via remote desktop—best suited to meet employee preferences and needs at any given time.

Meanwhile, dynamic Analytic provide data on who's using what, and when. These reports are readily available, and can be used to see who's logging in at various times and which apps they're accessing through Unified Workspace. This reporting tool can also be used by IT and operations to determine which third-party solutions are actually being used, and to identify opportunities to cut back on licenses for little-used apps.

IN SUMMARY

Unified Workspace unites disparate resources into one centralized work area, and all it typically takes is a day's worth of setup. Once configured by IT, users can get single sign-on access to all the apps and data they need—from any location and on any device. This on-premises or cloud hosted workspace aggregator resolves many common IT challenges by:

- Eliminating the need for VPNs to remotely access internal resources
- Creating a consistent user experience across devices, browsers and operating systems
- Leveraging existing directories to control role-based access
- Allowing new apps to be added within minutes
- Providing better access without compromising security
- Empowering users with more choice related to apps, devices and locations

"We were up and running in two days, including the training. It takes a PC and gives a consistent unified presence across platforms, whether you're Mac or Windows XP, Windows 7, Windows 8, tablet, iPad–whatever. It's been an easy way to give cross-platform access to the information our staff needs."

—Brian Churchill, Director of Information Systems, Sturdy Memorial Hospital

Additional Information

For browser requirements, supported databases and specifications, visit:

http://www.lenovosoftware.com/support/unified-workspace/specifications

---

Lenovo Unified Workspace empowers IT to deliver more flexible, agile and collaborative workplaces and meet evolving employee expectations. This workspace aggregator both modernizes and simplifies IT management with anytime, anywhere, any device access to public or private web-based apps, legacy Windows apps, remote desktops and file shares.

Lenovo is a $46 billion global *Fortune 500* company and a leader in providing innovative consumer, commercial and enterprise technology. Our portfolio of high-quality, secure products and services covers PCs (including the legendary Think and multi-mode YOGA brands), workstations, servers, storage, smart TVs and a family of mobile products like smartphones (including the Moto brand), tablets and apps.

Learn more at lenovosoftware.com/unified-workspace.