by the
numbers...

51%

51% of companies use or are considering using virtualization because of the flexibility with network configuration.
The 2020 State of Virtualization
https://www.spiceworks.com/marketing/reports/state-of-virtualization/

48%

48% of companies use or are considering using virtualization because of improved management capabilities.
The 2020 State of Virtualization
https://www.spiceworks.com/marketing/reports/state-of-virtualization/

45%

45% of companies use or are considering using virtualization because of improved security capabilities.
The 2020 State of Virtualization
https://www.spiceworks.com/marketing/reports/state-of-virtualization/

Why is VDI Important?

Virtual Desktop Infrastructure (VDI) is a revolutionary technology that many are familiar with but have never heard of. Words like "server" and "platform" can be confusing. To simplify it, VDI (virtual desktop infrastructure) is a central location (data center) where the computers are hosted. This might be a physical location within your office like a server room or an online cloud like AWS.

Users can remotely access their workstations and desktops from devices like thin clients, zero clients, tablets, or laptops. Some small and medium businesses think VDI comes with a high price tag and requires a dedicated IT department for implementation, discouraging them from introducing virtual desktops to their workplaces. All size businesses can get a lot of advantages from this technology and there are many ways to implement VDI on a budget.

Many companies are choosing to virtualize to save costs and be 'ready' in case they need to pivot fast because of natural disasters (like ice storms in Texas) or remote work demands (Covid 19 Pandemic) or simply because workers need to share proprietary information and are located continents apart (like research and engineering that has been globalized).

Increase Control Over Data

With data security becoming top priority for companies, VDI is becoming more important to cybersecurity efforts. Ask any cyber professional and they all agree that the cost to recover from a data breach is more expensive than prevention (https://www.nicitpartner.com/costs-cyber-security-prevention-vs-recovery/). Not only might there be a direct financial loss for paying a ransom there is also the lost production, dealing with reputation management, loss of customers, legal remediation, cleanup of files, and the future cost of training and maintaining good security.

Breaches happen for a variety of reasons and some can be prevented with VDI. A large health organization in Oregon had over 650,000 patient records exposes with a laptop was stolen from one of its vendors (https://healthitsecurity.com/news/computer-theft-exposes-personal-health-data-of-654k-oregon-patients).

A non-profit health system in Rhode Island paid over $1 million to settle potential violations after an employee's laptop that contained over 20,000 patients' names, medical records, and demographics; was stolen (https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html).

If your employees are issued a zero client or thin client and a keyboard, monitor and mouse, then the device can be stolen with no panic that data was breached. Even better, a zero client and thin client have no moving parts and can take the abuse of being shuffled around and there is no crying over spilled milk because these devices do not store data. They are only used to connect back to the virtual computer.

It is no secret that employees want to find a 'better mousetrap' while working and will download programs and applications that might aid them. The danger to

downloading is the potential virus that is lingering. Even with virus scan software, some malicious packages can take over anyway. This means that your employee has to trade out their device for a new one. With a zero client or thin client, the IT administrator can just swap out the infected computer for a fresh one. Even better, they have a recent backup so your employee doesn't lose productivity time. If your company has the resources, they hopefully caught the malware or virus before it even got that far with a good scanning process in place.

Centralize Support

The cost of managing updates and patches becomes more efficient with your employee's desktop virtualized. Imagine dozens or hundreds of employees that have to wait 45 minutes to an hour for an update to finish versus an IT administrator getting the alert and having those updates and patches finished by the time your employees log in. Security is also more strict when a dedicated IT administrator is monitoring and standardizing the process of updates and patches. When they go ignored, hackers have the ability to infiltrate networks and gain access to proprietary information. A cyber breach can occur simply because of neglect on single device. With all of the desktops located centrally, this job can become more efficient and effective.

With your resources centralized, your IT administrator is the new superhero and can be efficient and effective with their time and management of inventory.

Support and Scale Remote Work

The benefits of virtual desktop infrastructure (VDI) is providing mobility, security, and work freedom. With people changing roles and company requirements, VDI enables quick transition.

Mobility and flexibility is in high demand with employees. Between travel, working from home, or working from a secondary location, VDI in combination with a cloud means that employees are not bound to specific locations and can stay productive from different devices and pick up where they left off. With ClearCube's Cloud Desktop OS you can convert laptops into thin clients with a simple USB stick. You can send these home with contractors, vendors, students, employees, or freelancers to have access to your server or data center to complete projects or tasks and lets them bring their own device.

In a traditional PC setting, you would have to make application installations and software upgrades individually on each machine. VDI changes all that by allowing you to roll out quick updates to applications and operating systems. There is no need to test and prepare hardware and software configurations to make sure that they do not clash with your systems. This builds reliable IT systems as VDI brings uniformity across desktops and boosts productivity.

Be Ready for Disaster Recovery

Whether it is an accidental coffee spill, combating malware or corrupt files, businesses are aware that data loss is a cost that can range from hundreds to thousands of dollars. Disaster recovery goes beyond keeping

data safe. There are companies and businesses that do not have a choice of 'shutting down' because the services they provide are often critical during natural disasters. Having a backup in a separate data center or server allows employees to use their existing endpoint and switch quickly.

VDI delivers workforce continuity by completely transforming productivity and workflows. Every IT resource is has the ultimate goal of reducing costs and providing a high-quality end user experience. VDI delivers all the benefits of desktop and cloud technologies while enhancing security and the efficiency of organizations' IT resources.

Why ClearCube for VDI?

| Supply Chain & Manufacturing | Command & Control Centers | Government Agencies | Financial Services | Training & Education | Healthcare & Medical Technology | Engineering & Design | Department of Defense | Digital Signage | Oil & Gas | Small & Medium Business | Media & Entertainment |

ClearCube's expertise in virtual desktop infrastructure and specialization in endpoint devices combined with our data center experience allows us to quickly customize solutions for each and every business and organization that becomes a customer. Our highly specialized boutique services provide you with a tailored experience.