ComputerVault for a Post Covid-19 World

ComputerVault White Paper
May 2020

HCI / SDI / Private Cloud / Survey / SDN / VDI

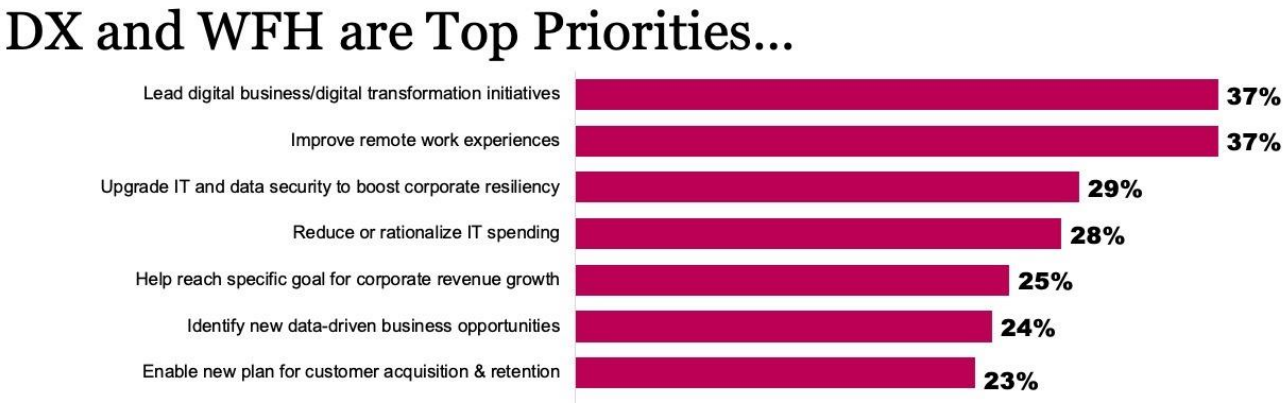
ComputerVault for a Post Covid-19 World

ComputerVault for a Post Covid-19 World

Surveys of IT Leaders by IDG Research and various publications, such as CIO, ComputerWorld, CSO, InfoWorld, Network World, have identified the priorities that these leaders believe IT organizations will face after the Covid-19 crisis:

1. Double Down on Digital Transformation
2. Improve the Work from Home Experience
3. More Security

Overshadowing these considerations, however, is the need to manage expenses and control costs. In general, most IT leaders expect IT spending to remain about the same or decrease in the coming months.



Digital Transformation tied with improving the remote work experience as the top priority among the IT leaders surveyed in the CIO COVID-19 Impact Study. IDG Research.

ComputerVault HCI

- **Lowest TCO**
- **Highest Security**
- **Best Performance**
- **Drives Digital Transformation**

One of the important considerations to keep in mind, however, during a crisis that is paralyzing businesses and society, is to avoid the trap of delaying digital strategy decisions. It is common for organizations in this situation to continue with the existing ways of doing things and focus only on business resiliency.

Doing so may cause businesses to miss an opportunity because of the pent-up demand which is expected to result in enormous spending once the crisis ends. Businesses need to be in position to take advantage of this spending. Now is the time to focus on technology initiatives.

ComputerVault HCI drives digital transformation by ensuring that all corporate data and resources are available to all users at all times regardless of the location of the users, data and resources.

ComputerVault Hyper-Converged Infrastructure includes:

- Hyper-converged Infrastructure optimized for COTS hardware
- Zero Trust Security Model that stops malware and phishing
- Virtual Desktops & Servers
- IoT Edge to Core Management
- Video Conferencing

Digital Transformation

Every IT organization struggles with how to improve the competitiveness in the face of rapid change. Organizations that make the most important advancements during the current downturn, are the ones that will win in the recovery.

Using ComputerVault HCI, corporate data is accessible to all users at all times:

- Regardless of where the Data resides
- Regardless of where the User is working
- Regardless of where the Applications are hosted

This means that organizations may host resources and data where it is most advantageous, while providing granular access to their users, partners, vendors and supply chain. Moreover, users are free to use any device, i.e., PC, laptop, phone, tablet, etc., with a browser, to connect to their virtual desktops and access corporate resources and data wherever the Internet is available.

Improve WFH Experience

Most businesses expect that working from home will play a larger role for their workforces in the future. However, doing so challenges remote networking, IT support and cybersecurity. The lack of sufficient VPN connections is the biggest infrastructure issue businesses face.

ComputerVault Virtual Desktops make working remotely or from home just like being in the office. First, it *is* the user's work desktop. It has all the software, tools and applications the end-user needs installed and configured. Since the virtual desktop is hosted within the corporate infrastructure, it is centrally supported and secured by the IT organization.

There's no data on the end-user device either. All corporate data and files remain in the corporate infrastructure. The ComputerVault Virtual Desktop

provides access to those resources, data and files, but they never leave the datacenter.

ComputerVault WFH

- **Just like being in the Office**
- **Central IT Support**
- **Data Always in Datacenter**

A ComputerVault Virtual Desktop performs faster than a PC or laptop on your desk. This is true when the user is in the office or when working remotely.

With all the applications, data and resources available to the user regardless of location and with performance that is better than a physical PC or laptop, users are just as productive when working remotely as they are when in the office.

Organizations are secure in the knowledge that corporate files, data and intellectual property never resides on the end user devices, and that IT is centrally managing security.

Lastly, the built-in ComputerVault VPN with Multi-Factor Authentication, means that no third-party hardware or solutions are required for accessing corporate resources. All that is require is inexpensive, abundant broadband Internet. This reduces both cost and security vulnerabilities.

Improve Cybersecurity

Working from home increases endpoint vulnerability. That's an unavoidable fact. According to Trustwave, ransomware and cloud attacks more than doubled in 2019. According to "Forrester's Guide to Paying Ransomware," released in June 2019, ransomware attacks increased 500% over the prior year and Forrester estimated that the attacks will cost businesses $11.5 billion in 2019. Phishing attacks have seen a 350% increase since the Coronavirus Crisis began, according to Google, because hackers and cyber-criminals know that more people are working remotely.

With workers out of the office, more of the security burden falls on. Protection and assistance from the IT organization is more difficult, and hackers and cyber-criminals are attempting to take advantage of the situation.

The reality is that physical end-user devices, such as PC's, laptops, phones, tablets, etc., can never really be secured, and they all have vulnerabilities. Lastly, end-user can be and will be fooled.

The only solution to this is to use a true Zero Trust Security Model since it assumes that all end-user devices are compromised. With ComputerVault, an end-user device compromise does not affect corporate resources, intellectual property, data or files.

Zero Trust Security Model

The Zero Trust Security Model requires strict identity and device verification, regardless of the user's location in relation to the network perimeter. This is unlike the traditional approach to network security, known as the castle-and-moat model, where once inside the firewall, users are automatically trusted.

ComputerVault

- **True Zero Trust**
- **No Up/Down-Load**
- **Data Isolated**

ComputerVault prevents malware infections and stops phishing attacks by isolating corporate resources, data, files and IP from the Internet. Data and files can't be downloaded to end-user devices, maintaining data privacy. If end-user devices are lost or stolen, there is nothing of value that can be retrieved from them.

No upload from end-user devices is permitted to the virtual desktop, either. If an end-user device is infected with malware, that malware cannot reach the corporate infrastructure. As endpoints are not connected to each other, the infection cannot spread. Infected devices are merely unplugged and replaced with a new device. The infected device is wiped clean and the software reinstalled so it can be used again.

ComputerVault recommends that end-users browse the Internet with their client device and expose it to the internet, as no harm occurs if it is compromised. The ComputerVault Virtual Desktop will however, provide access to known, safe websites and domains that are required for work.

Manage Expenses and Reduce Costs

Most businesses expect IT budgets to be flat or decline after the Covid-19 crisis. Any budget increases will be small, and IT organizations are expected to do more with less. ComputerVault HCI offers several advantages in these circumstances.

First, ComputerVault has a lower Total Cost of Ownership than any competing virtualization product. ComputerVault has a lower TCO than buying and supporting PC's and laptops. In fact, ComputerVault is 1/3rd to 1/6th the cost of competing products, for several reasons:

1. ComputerVault is 100% Proprietary (licenses no 3rd Party software)
2. Optimized for COTS hardware
3. Subscription Licensing with 24x7 Support Included

Using Commercially Available Off-the-Shelf servers and hardware further reduces capital expenditures and lowers TCO. Utilizing hyper-converged infrastructure delivers flexibility to consolidate legacy systems and the opportunity to lower fixed operating costs as well.

Remote support for ComputerVault HCI, is included in the subscription. Customers do not need to hire software administrators. ComputerVault supports the entire technology stack 24x7 as part of the software license.

ComputerVault

- **Lowest TCO**
- **Shift CapEx to OpEx**
- **24x7 Support**

The technology stack does not require buying and installing any other software to make ComputerVault work. Competing solutions license software from 3rd parties, passing those costs on to customers. Those solutions usually require installing other separately licensed software to enable features such as virtual desktops, further driving up costs.

ComputerVault HCI is installed from a DVD or image and an environment can be deployed in a few hours. Because of its performance, ComputerVault may be deployed wherever it is most advantageous, i.e., on-premises, cloud, colo, datacenter, etc., regardless of the location of end-users and corporate resources.

Conclusion

The focus of CIO's moving forward is:

- Double down on Digital Transformation
- Improving Remote Work experience
- Focus on Cybersecurity management
- Manage Costs

ComputerVault provides the technology roadmap to deliver increased competitiveness and flexibility while reducing costs for the "Next Normal."

References

1. ComputerVault Hyper-converged Infrastructure (HCI), ComputerVault, Inc., white paper, (Available Upon Request)

2. Exclusive survey: What 400 IT leaders really think about the COVID-19 crisis, CIO, https://www.cio.com/article/3541508/exclusive-survey-what-400-it-leaders-really-think-about-the-covid-19-crisis.html

3. Doubling down on digital transformation during the coronavirus pandemic, CIO, https://www.cio.com/article/3533993/doubling-down-on-digital-transformation-during-the-coronavirus-pandemic.html

4. A practical way for CIOs to manage IT Costs trough the COVID-19 Crisis. McKinsey Digital, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-practical-way-for-cios-to-manage-it-costs-through-the-covid-19-crisis

5. Rise in ransomware attacks prompts new prevention priorities, Tech Target, https://searchsecurity.techtarget.com/feature/Rise-in-ransomware-attacks-prompts-new-prevention-priorities

6. Ransomware, cloud attacks more than doubled in 2019, Tech Target, https://searchsecurity.techtarget.com/news/252482012/Ransomware-cloud-attacks-more-than-doubled-in-2019

7. Google Data Reveals 350% Surge In Phishing Websites During Coronavirus Pandemic, Forbes, https://www.forbes.com/sites/jessedamiani/2020/03/26/google-data-reveals-350-surge-in-phishing-websites-during-coronavirus-pandemic/#691665af19d5

ComputerVault for a Post Covid-19 World
May 2020
Published by ComputerVault, Inc.

Authors: Paul Angelo, Peo Nathan, and Shanmugha Bharathy Balasubramaniam, ComputerVault, Inc.

ComputerVault, Inc.
65 Boston Post Road W
Marlborough, MA 01752
U.S.A.
www.ComputerVault.com

Inquiries:
Phone: +1.508.624.9900
Fax: +1.508.624.9905