Productivity Enhancement and Protection
Improving Business IT Resilience
Computer Desktop Fallback

2024-04-10

Problem Needing To Be Solved

On conventional business IT systems, by the time you detect signs of a breach it's almost certainly too late to prevent major operational flow disruption and big costs.

Unsurprising in view of some BigTech appearing to prefer charging you subscriptions for services to alert you to problems happening instead of eliminating the problems.

Microsoft's annual income from 'security' subscriptions now exceeds USD 20 billion, and yet the plague of invasions of Windows-based business IT systems (including Microsoft's own systems) continues apparently unabated. As security expert Kevin Beaumont has commented “Microsoft is the world leader in monetising its failure”.

When malware invades business IT systems almost all of them rapidly get every server and every desktop disabled.

The situation has been likened to having a sudden heart attack followed by needing open-heart surgery.

The full effects of sudden blood or data flow disruption are grossly underestimated by most. Problems can easily persist for months.

Maintaining operational flow is what really matters, and we can deliver that for you.

Our approach is unique in that we expect malware to invade a business's IT system. But the business continues running regardless, due to the benefits of the technology and techniques we provide that keep operational data flowing.

Imagine how comfortable you and the rest of your staff will feel once you all know how little effect a Windows malware outbreak can have with our solutions in play.

Action is needed to increase the resilience of both servers and desktops. Our Malware Defeating File Sharer (MDFS) solves the server resilience problem.

Simply reinstalling and configuring affected Windows desktops is time-consuming and highly disruptive and so something better is needed.

Optimum Desktop Resilience Solution

The aim must be to be able to continue doing all necessary actions after Windows machines have been disabled by malware, and with the malware still present on the system and searching for new victims.

The optimum solution is to also have available desktops that are immune to Windows malware, and have enough of them to ensure that all necessary operational flow actions can be performed. Many alternative (non-Windows) desktops provide the same or equivalent functionality as Windows desktops.

Optimum Implementation

The optimum implementation involves having Virtual Machines on each desktop machine, plus a Hypervisor installed to run them. One VM runs its Windows Desktop (existing or new) and another VM runs an Alternative Desktop.

Like humans in general, some IT people resist change and so consider the use of VMs to be an unnecessary complication.

But in this case they deliver a major simplification - when Windows malware strikes it affects only the Windows VM and not the entire machine.

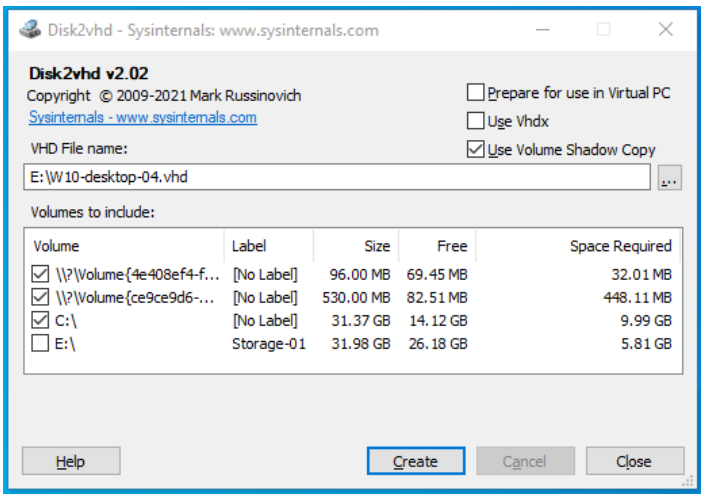
After the machine has booted the user chooses which VM to run. When the Windows Desktop becomes non-operational they simply switch to the other one and continue work.

If a machine has sufficient memory (RAM) the two VMs can be run simultaneously. Switching between them is quick and easy via keyboard hot-keys.

Warning : *Do not create dual-boot machines instead, because that arrangement makes the files of the alternative system vulnerable to attack by Windows malware.*

Other benefits of moving to VMs include making more efficient use of computer hardware, and being able to set up new VM(s) on machines whilst they're running existing VM(s).

Conversion Of Existing Windows Desktops to VMs



Conversion is quite straightforward using the free program Disk2VHD that's downloadable from Microsoft.

When run on a Windows machine it creates a VHD (Virtual Hard Disk) file containing everything from the installed system.

Create the VHD version because VirtualBox can't use VHDX.

You'll need to connect a removable storage device for Disk2VHD to save the VHD file on.

Alternative Desktops

We use and recommend the Linux-based MATE (mah-tay) desktop, which is very easy to use even for people unfamiliar with non-Windows desktops.

MATE is a continuing-development of an earlier desktop paradigm.

It retains drop-down menus on the desktop which makes it easy for new users to find things.

Getting to grips with it is easier than getting to grips with a new car.

The standard MATE desktop installs contain a lot of application software. Including the Firefox web browser and LibreOffice. The latter can handle MS Word documents and Excel spreadsheets. It's also very simple to connect them to Windows file shares, and to printers.

This document has been produced on a Fedora Linux MATE desktop using LibreOffice. The desktop's 'Connect to server' facility is used to copy the LibreOffice-generated PDF version of it to our web server. The copying is done via the familiar drag-and-drop action. The connection is set up seamlessly by the desktop's Caja file manager, and is authenticated and highly secure (SFTP), and it protects both the server and the desktop.

Again, some IT people might think it an unnecessary complication. We're familiar with MS Windows via using it for compatibility testing and find it cluttered and relatively tedious when trying to 'get stuff done'. It's great to get back to MATE with its easy-to-switch-between multiple desktop spaces and easy-to-find-and-use programs. It's also a much quieter work environment than MS Windows. Some of your staff may come to prefer it over Windows for being productive.

Fedora Linux contains bleeding-edge software. New versions are released at 6 month intervals, and it has a very simple and reliable upgrade-in-place process. Several desktop variants are available, with MATE being one of them.

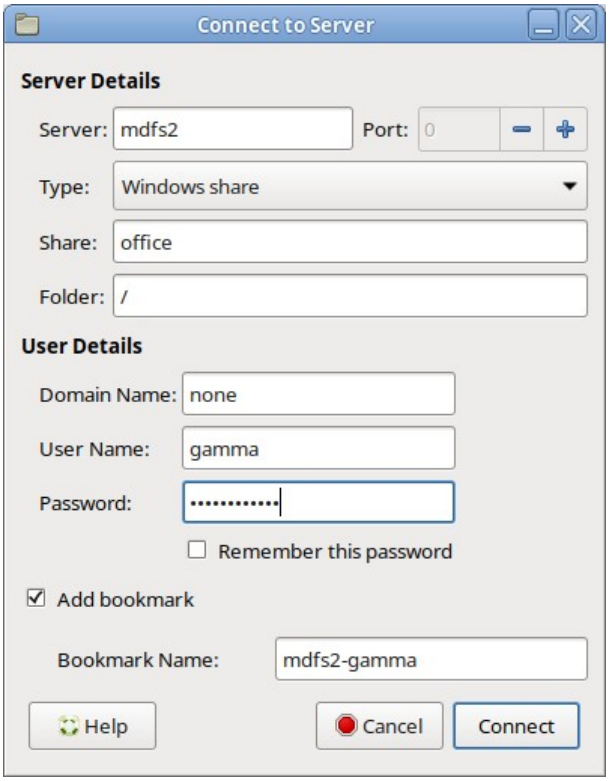
Visit: https://spins.fedoraproject.org/mate-compiz/download/index.html

AlmaLinux and Rocky Linux are Enterprise Linux versions with long-term-support. Version 9 is the latest and it's supported until 2032. Several desktop variants are available, with MATE being one of them.

Visit: https://docs.rockylinux.org/guides/desktop/mate_installation/

Note that Microsoft has joined the game by publishing a guide to downloading and installing Linux-based systems, but we recommend sticking to documentation provided by the creators of the systems.

Connecting the MATE Desktop to File Shares



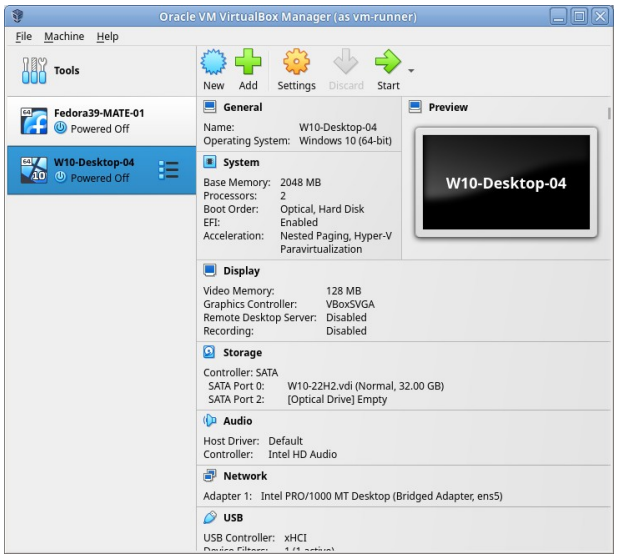
If you've previously connected to a share and have saved a bookmark for it, then open the Caja file manager and click on the share's bookmark in the sidebar.

To connect to a share for the first time, click on the desktop Places menu and then 'Connect to server'. In the window that appears change Type to 'Windows share', and then enter details in the expanded window. Since we advise not joining Alternative Desktops to domains, enter None in the Domain Name slot.

It's possible that in the dark recesses of MS-Windows there's a setting that requires a valid domain name to be supplied when connecting to a Windows server even in a case like this. If you can't connect and everything else in the form is definitely correct then as a last resort enter a valid domain name.

Note that our MDFS doesn't require a valid domain name to be entered for connecting to its shares.

Hypervisor



We use and recommend VirtualBox 7, run by minimal installs of AlmaLinux 9 or Rocky Linux 9.

Visit: https://www.virtualbox.org/wiki/Downloads

Shown is the VirtualBox 7 GUI as seen on a MATE desktop that's configured to use traditional styling.

The GUI is not usable on Desktop Fallback machines, for security reasons. You use it on the VM Maintenance Machines.

Warning : *Avoid using Microsoft HyperV, because it runs on Windows only, making it vulnerable to attack by Windows malware.*

Converting Your Business To Desktop Fallback

Important : All machines that are to run VMs need to have Hardware Virtualisation enabled in their BIOS settings.

On your main office network reserve a block of IP addresses for the Hypervisor layer of machines, and give each Hypervisor layer instance a fixed (static) address from that block, and exclude that block from allocation by the DHCP server. If possible set up DNS entries for them so that they can be referred to by name.

All the necessary software components involved are free to download and use, so you can do the whole thing yourself. However, after installation a variety of configuration changes and other customisations are required for both the Hypervisor layer and the Alternative Desktop VM.

In particular the Hypervisor layer should display the names of the available VMs and allow the user to select which one(s) to start, and that functionality needs to be safe and secure.

In our implementation of that, the desktop user logs-in as user vm-starter, but the VMs are owned and controlled by user vm-runner. The graphical program run automatically after user log-in sends user-initiated requests to vm-runner, and such requests are limited to getting lists of VMs (available and running), and starting a particular VM.

If you have Windows Servers then changing to running them on VMs also has major resilience benefits. We recommend our standard Hypervisor setup for those too.

As an alternative to doing it yourself, we provide a remote service that installs a customised version of our standard Hypervisor on a machine (Desktop Fallback, Server). Note that prior to installing on machines that have Windows installed you need to have used Disk2VHD to create a VHD of the installed Windows on a removable storage device - and preferably verified that it works.

Our service can also provide customised Fedora/Rocky MATE Desktop VMs, and remote installs of VM Maintenance Machines. The business value of the resilience-increase far exceeds the cost of the service. Contact us for details of the service : https://iopen.co.nz/ws_contact.html

With our service, for the Hypervisor and VM Maintenance Machine installs you boot the machine from a USB flash stick (4GB minimum) whose contents we provide as a .iso file. You use a free program called Rufus (https://rufus.ie/en/) to get it written to the flash device. The resulting Fedora MATE Desktop system creates a VPN connection to our server and via that VPN tunnel we do the install.

Alternative Desktop Familiarisation

We recommend that users become familiar with using the alternative desktop before they have to use it. Preferably by using it to do actual business work. So there'll be little interruption to their normal workflow when Windows malware invades.

If a desktop machine has at least 8 GB memory (RAM) it's feasible to run the 2 VMs simultaneously, and it's simple to switch between them using keypresses. With both running perhaps do some of your work on one VM and the rest on the other.

Instead of shutting down a VM you can click on the VirtualBox window's close symbol and choose “Save the machine state”. That way, when you restart the VM you'll be exactly where you left off.

For 8 GB RAM allocate 4 GB to the Windows VM and 3 GB to the Linux one, thus leaving 1 GB for the Hypervisor. If more than 8 GB RAM then allocate 4 GB to each VM.

Recovery Following Malware Invasion

Create replacement Windows VMs. The most reliable way is to create such VMs on one or more dedicated machines (see the VM Maintenance Machines section below) and to copy each VM to the appropriate machine via the network. That way you automatically retain a copy of each VM, as initially set up. Staff continue to work on the Alternative Desktop VM whilst all that is happening, and can switch to the new Windows VM when appropriate.

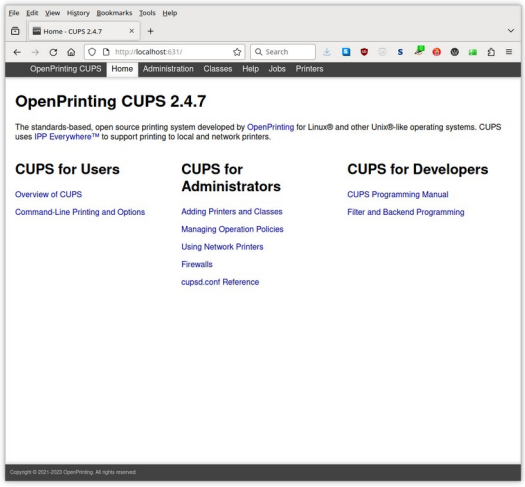
You can create replacement Windows VMs ahead of time. But after malware invades, before using any of them be sure to eliminate from your entire IT system both the malware and the vulnerability which allowed it to get in. If the replacement Windows VMs need to be updated then do it on the VM Maintenance Machines.

Further Resilience-Increasing Actions

Some of these are about eliminating dependence on Windows machines (especially Domain Controllers) for essential network functionality, so that when they get taken down by malware your networking is unaffected.

Ensure that all of your DNS and DHCP servers are hosted by non-Windows machines.

Avoid joining Alternative Desktop VMs to a domain. Instead simply get them to connect directly to file shares.



If any printers are connected to Windows machines then disconnect them and make them accessible via your LAN.

If a printer doesn't have a network interface then a good approach is to use a Raspberry Pi (or similar) computer as a CUPS-based printing server and connect the printer to one of its USB ports.

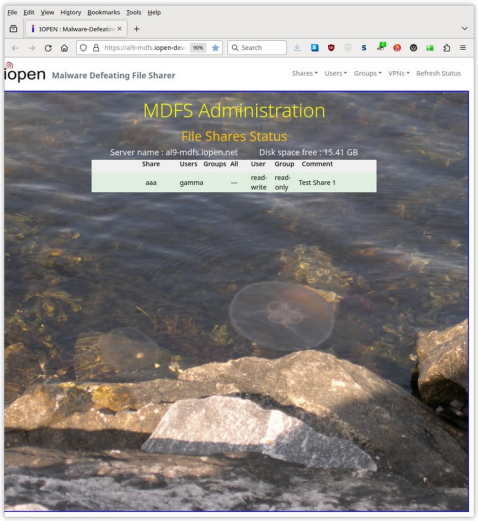
If two or more such printers are located close to each other then a single RPi can handle all of them. Installing and configuring CUPS on RPi is well documented online.

Our printing is handled by an RPi version 1B (2012), which does several other things as well.

CUPS was formerly an acronym for Common UNIX Printing System.

CUPS is based on IPP (Internet Printing Protocol). For simplicity we recommend connecting Windows desktops via IPP to CUPS-managed printers rather than via Windows SMB networking. Linux desktops generally prefer IPP.

If you can run both VMs simultaneously then you can decide how much downtime there'll be when Windows malware strikes. Because the components of your workload that you move to the Alternative Desktop will be unaffected when Windows malware strikes. Provided the data used by those components isn't accessible to the malware.



If also using our Malware Defeating File Sharer (MDFS), consider creating shares on it that only Alternative Desktop users and groups can access, so Windows malware can't affect the files stored in those shares.

Defence in Depth.

Avoid using 'The Cloud' for important things (data or operations) because there's many ways it can go wrong. And when something does go wrong your options are very limited.

Resources stored in 'The Cloud' are vulnerable to both direct and indirect attack. If any of your local Windows machines are connected to remote resources when Windows malware strikes, then it's possible that those resources can be attacked when the malware invades the connected machines.

You can outsource the work but you can't outsource the risk.

With competently set-up local systems the total cost over time will be significantly lower and the reliability significantly better, and there'll be no ongoing subscriptions.

Furthermore, you don't need so-called 'Enterprise Grade' hardware in order to get good performance and reliability and resilience.

So keep your operating-data close and your backup-data safely close.

See also : https://iopen.co.nz/docs/total_cost.pdf

VM Maintenance Machines

Note that our remote install service includes installing on Maintenance Machines.

Moderate hardware requirements : Modern fast CPU with a lot of cores and built-in graphics; at least 32 GB RAM; Gigabit wired network interface; at least 2 USB3 or USB-C ports; enough disk storage to hold all the VMs. To minimise SSD wear the latter disks can be the USB-interface removable type. Use 2 - one as primary storage and the other for backups. Connect them to USB3 or USB-C. If possible buy machines with no OS installed. Using 'spare' display, keyboard, mouse will be fine.

In NZ, PBTech (https://pbtech.co.nz) often offer what they call 'Intel Upgrade box (no OS)' which is almost certainly suitable. Due to absence of OS (i.e. MS-Windows) its cost is likely to be below the NZ CapEx threshold even after adding RAM to it.

The one we bought was well below the CapEx threshold even after adding 16 GB of RAM (for 32 GB total) and a Gigabit Ethernet card. We routinely have it running 7 VMs, and there's still plenty of unused resources. It's one of these :

https://www.pbtech.co.nz/product/WKSPB14509/PB-14509-Intel-Upgrade-Box-Intel-Core-i5-12400-6-C

Depending on the number of Windows machines that you need to set up VMs for, it may be advisable to have more than one Maintenance Machine (MM). The speed limiting factor will probably be disk writes.

Details are in the separate document https://iopen.co.nz/docs/vm-maintenance.pdf

Summary :

- Use a separate network (e.g. 172.18.1.0/24) for the MMs and the VMs on them.
- Use a gateway router and connect its upstream network port to the main office network, and set up a DHCP server on its downstream side configured to allocate addresses in the range 172.18.1.128 .. 254 (for the VMs). On all VMs be sure to set Network to 'Bridged Adapter'.
- Give the router's downstream side the first host address (172.18.1.1).
- Give each MM's Hypervisor layer an address from the range 172.18.1.2 .. 15
- Configure the router to

  Block all connection attempts from upstream, so that malware on the main network can't attack VMs being run by the MMs.

  Block attempts by VMs on the MMs (addresses 172.18.1.128/25) to connect to machines on the main network (such as Domain Controllers), but allow them to connect to wherever they download updates from.

  Allow MMs (addresses 172.18.1.0/28) to connect to anywhere, so that they can copy VMs to/from the Hypervisor layer of machines on the main network, and download updates.

- On the MM machines install and configure Fedora MATE plus VirtualBox 7.
- On the MMs use the MATE 'Connect to server' function to copy VMs to/from the Alma/Rocky Linux Hypervisor layer of machines on the main network.

Our Motivation For Producing This

We want businesses to achieve better outcomes, regardless of whether we're directly involved in making them happen. Such outcomes can produce effects that benefit many, including ourselves.