Malware Defeating File Sharer
Terms and Conditions

2023-06-17

Supercedes all earlier versions E&OE.

Definitions

In the following : 'we', 'us' and 'our' refer to IOPEN Technologies Ltd; 'you' and 'your' refer to the client; 'authorised' means authorised by us; 'our associates' refers to third parties authorised by us.

Product Scope

Malware Defeating File Sharer (MDFS) is a software system, which we install remotely on suitable hardware either provided by you or otherwise supplied to you. We are responsible only for our software components and the configuring of the system.

MDFS is supplied as a Virtual Machine (VM). See Note 1.

Warranties

Hardware warranties are the responsibility of the hardware supplier.

Base system software packages have their own warranties.

We will fix non-excluded problems in our software on your system remotely without charge for a period of 1 year from your system starting to be used.

Requirements for your premises

MDFS machines must be physically secure - in a locked room and/or a locked cabinet.

MDFS user data and monitoring data must be backed-up frequently automatically securely, because hardware failure is always a possibility. See Note 4.

The machine running the MDFS VM must be connected to your internal network via a Cat5e or better Ethernet cable. With internal network speed being at least 1 Gbit/s.

An Internet connection fast enough to make remote support and software installation and upgrading efficient, and (if you use that option) fast enough for usable-enough remote access to file shares, and for making off-site backups of data files. See Note 6.

Payment

Payment for your MDFS system is due by the 20th of the month following that in which it started to be used.

Software Licences

The system bases are comprised of sets of software packages from an Enterprise Linux (EL) distribution, and the individual package licences apply. See Note 2.

Components created by us are licenced to you specifically. A major reason being protection against the appearance of insecure or backdoored versions of them.

Software Support

We and our associates can provide software support remotely via a secure VPN.

Non-warranty support can be via either support contract or per-instance charging.

Software Updates

Base system software package updates are done automatically and securely via the standard EL mechanism soon after 03:00 (local time) each day. A few package updates require a system or VM reboot in order to take effect, and when necessary that will be done automatically after updates installation is complete. See Note 3.

Updates to our software components are done via download from our secure web server. The MDFS system checks daily for updates. We can also update via the support VPN.

Administration of Low Level Aspects

Low level access is restricted to being via a secure VPN, and it must be done using only non-MS-Windows computers.

A standard MDFS machine has a secure VPN client which connects to our secure VPN server. On our server we enable it for your machine only during system setting-up and when support operations are needed. See Note 5.

Limitations

No computer can be completely secure, and we do not claim that MDFS is. If operated according to our stated conditions then it will be very hard to make it fail to function as required.

Detection of file exfiltration is necessarily imprecise, so we claim only to provide best-effort detection. As part of the process our software analyses your file accessing to derive your typical access patterns. We sometimes send information about your file accesses to our server (securely) for further analysis, but we never send any of the actual files.

An MDFS machine can be joined to an MS-Windows Domain if necessary, but we will not enable GPO (Group Policy Object) functionality, since it is often abused by Windows malware. For reliabiliity we recommend avoiding joining it to a domain if at all possible so that it remains fully usable when your Domain Controllers get taken down.

Disclaimer of Liability

Because we have no control over what happens on client premises we accept no responsibility for unwanted occurrences related to MDFS. Including, but not limited to, any problems that appear following :

(a) non-authorised person(s) physically accessing the hardware

(b) non-authorised changes made to low-level settings

(c) low level access from computers running MS-Windows

(d) inadequate backing-up of data.

Furthermore, any network connectivity problems that occur when the local network's DNS or DHCP servers are run by Windows machines.

Refund Policy

MDFS is based on mainstream technology, has long-term viability, and clearly provides MS-Windows-compatible file sharing, plus Windows Domain functionality when necessary.

We can provide free test-drives of the MDFS system to enable potential clients to become fully familiar with it. Futhermore, our support capabilities are second to none.

So we can't imagine a situation where a refund would be justifiable.

As stated earlier, the hardware is the responsibility of the hardware supplier.

Notes

These notes provide explanations and some further conditions :

1 : The MDFS VM's operating system is an Enterprise Linux (EL). The VM is required to be run by an EL-based machine with VirtualBox version 7 as the Hypervisor. The machine's EL variant must have SELinux running in Enforcing mode. If necessary we will remotely install EL and VirtualBox on suitable hardware.

The MDFS VM must have a static IP address and its hostname needs to DNS-resolve to that address. The DHCP and DNS servers involved should not be hosted on an MS-Windows machine, because Windows-hosted servers are likely to be affected by a malware outbreak.

For safety, an MDFS VM **must not** be run by a Hypervisor on an MS-Windows machine, because doing that makes it possible for Windows malware to attack VM files.

2 : Currently we use AlmaLinux 9 and Rocky Linux 9, and typically their packages use an Open Source licence.

3 : AlmaLinux 9 and Rocky Linux 9 are supported until 2032. Version 9 is the latest. The MDFS VM's structure makes it straightforward to upgrade to a forthcoming version, if needed.

4 : Backing-up of data must be done frequently and automatically. Backing-up of files on MDFS shares must not be done via normal Windows-type access to the shares because the file accesses involved are indistinguishable from workstation malware doing file exfiltration.

Backing-up must be done using a 'pull' mechanism and via a secure VPN connection. See Notes 6 and 7. The backup and restore processes must not involve any MS-Windows computers.

5 : The Support VPN : We have your support VPN enabled only during support sessions for you. Your MDFS system can determine whether its support VPN client should be enabled, and its Adminstration web server can show you whether it's currently enabled or disabled.

If you must have more control of VPN access you can use your network gateway's firewall to enable/disable VPN data flow, in which case we will supply details of the relevant settings. Note that if you do that, then in the event of a problem an appropriate member of your staff will need to enable VPN data flow promptly.

6 : Remote Access to File Shares and the making of backups of files : The MDFS machine runs one VPN server that provides secure remote access to its file shares, and another that provides the backup channel. We will supply configuration details when their use is required.

2023-06-17

Notes

7 : The generating and distributing of VPN keys :

For each machine needing remote access to file shares, and each machine doing file backing-up, a VPN client has to be installed on the machine, and a key pair (public + private) generated and installed. Private keys must be kept secure. The VPN client needs the client's private key and the VPN server's public key. The VPN server needs the client's public key.

The latter item requires low level administrative access to the MDFS VM and if done by you must be by an experienced authorised person and from a non-Windows machine. If you do not have a suitable experienced person then we can do it remotely via the support VPN. If you have a support contract then the cost may be covered by that. Otherwise our normal support chargeout rate applies. For efficiency and cost minimisation you may wish to get several VPN client public keys installed on MDFS VPN servers in a single support session.

8 : Use of non-Windows computers :

We require non-Windows computers to be used for some things. One of the reasons is to defend against criminals adding functionaility to Windows malware that enable an infected Windows machine to make undesirable changes to any machine that it's used for low-level administrative access to.

There is an IT resilience aspect to having at least two non-Windows Desktop machines on hand, since they will remain fully operational when your Windows machines get hit. To achieve that we recommend installing Fedora Linux on spare PC(s). The MATE desktop variant is very easy to use.

For your protection and ours we require you to provide us with a signed copy of our latest MDFS Terms and Conditions before we deliver a system. A scanned image of the signed copy is acceptable.

We the client have read and understood the foregoing MDFS Terms and Conditions and hereby accept them :

Date :

Client's Legal Name :

Representative's Function :

Representative's Name :

Representative's Signature: