



Malware Defeating File Sharer Terms and Conditions

2023-05-03

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. 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 tries to establish that VPN connection to our VPN server, and on our server we enable it for that 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. As part of it our software analyses your file accessing to derive your typical access patterns.

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 reliability we recommend not joining it to a domain if at all possible.

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-authorized person(s) physically accessing the hardware;
- (b) non-authorized changes made to low-level settings;
- (c) low level access from computers running MS-Windows;
- (d) inadequate backing-up of data.

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

Refund Policy continued ...

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 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 via you getting a static lease for it created on your DHCP server. The hostname of the VM needs to be made to DNS-resolve to that address.

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 its Virtual Hard Disk 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 automatically. User-data backing-up must not be done by any of your user machines as 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 network connection.

The backup and restore processes must not involve any MS-Windows computers.

5 : The Support VPN : We have our end of your support VPN enabled only during support sessions for you. Pursuant to the Principle of Least Access,

If you must have direct control of 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 data flow promptly.

6 : Remote Access to File Shares : The MDFS machine runs a VPN server that provides secure remote access to its file shares. We will supply details when its use is desired.

IOPEN Technologies Ltd (NZ) - <https://iopen.co.nz> & <https://iopen.net>