How to install and use Microsoft Defender in Linux

While many Linux users outside the enterprise may not fully understand the importance of Microsoft tools on Linux, those inside will certainly understand that they can be invaluable.

Integration with Active Directory and much of the Microsoft ecosystem is huge for desktop Linux, and it could make your favorite distribution a more viable operating system at work. . One of the most important parts of the business is security. This guide will show you how to install and use Microsoft Defender on Linux to make sure the IT department can scan your machine and look for threats.

How to install Microsoft Defender in Linux

To install Microsoft Defender on Linux, the instructions will differ depending on the distribution. Microsoft hasn't put its packages in repositories yet, so you'll have to make sure you install the right dependencies and add the repositories.

The distribution is based on RPM

You will need **yum-utils** or **dnf-utils** :

```
sudo dnf instll yum-utils
```

To configure Microsoft repos, the basic syntax of Microsoft repos is as follows:

```
https://packages.microsoft.com/config/[distro]/[version]/[channel].repo
```

Posts will use **prod.repo** , because all distributions are available **prod.repo** or **prod.list.** So for Fedora systems that command would look like this:

```
sudo yum-config-manager --add-repo=https://packages.microsoft.com/config/fedora/
```

For CentOS systems, the command will be as follows:

```
sudo yum-config-manager --add-repo=https://packages.microsoft.com/config/centos/
```

The example is using the yum command as it is targeted at RHEL, CentOS, and Oracle Linux, but you can use dnf as well. You will also need to enter the Microsoft GPG key with the following command:

```
sudo rpm --import http://packages.microsoft.com/keys/microsoft.asc
```

Run quick update:

```
sudo yum update
```

After that, you'll just need to install the package called **mdatp** or **Microsoft Defender Advanced Threat Protection** .

```
sudo yum install mdatp
```

Debian / Ubuntu system

You will need some additional dependencies:

```
sudo apt install curl libplist-utils
```

Then you can basically follow the same process:

```
curl -o microsoft.list https://packages.microsoft.com/config/ubuntu/20.04/prod.li
```

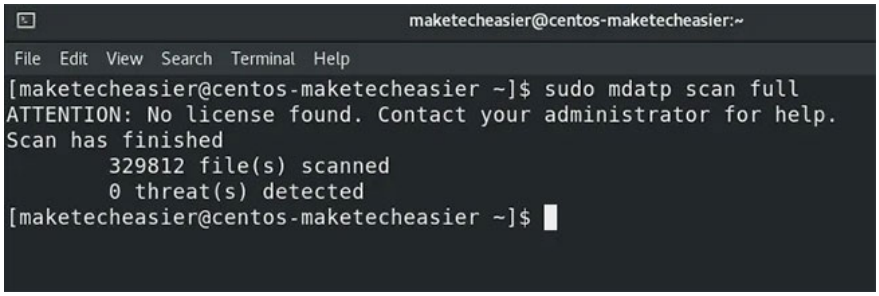
Install the repo, GPG key, all dependencies and mdatp.

Use Microsoft Defender on Linux

Run a scan for threats

One of the main things you may want to do is scan your system for threats. To do that, open Terminal and type the following command:

```
mdatp scan full
```



This will scan all files it has access to (in our case 329,812 in our case) and report any threats it knows about. You can also run quick scans or custom scans. Customization options allow you to specify a directory or file, or to ignore any exceptions that you have previously set. You can run the scan as follows:

```
mdatp scan custom --path /PATH/TO/DIRECTORY --ignore-exclusions
```

If you have set an exclusion as mentioned below, you can run the scan above.

Update virus signature

To update the signature virus on Microsoft Defender on Linux, update it like any other package.

```
sudo yum update mdatp sudo apt-get upgrade mdatp
```

Set exclusion

To exclude deemed good files from being reported, there are several ways you can do it. To exclude a file type, you can use the following command:

```
mdatp exclusion extension add --name .png
```

This will select all the .png files and put them in the exclusion list. If you have a specific file type created by you and know that you will never need a scan, you can use this command to do so.

To exclude a directory, you can use a similar command:

```
mdatp exclusion folder add --path /PATH/TO/DIRECTORY/
```

Now, any folder you have just asked for the **mdatp** to exclude will not be scanned. This is very useful if you have some security testing tool on your system.