

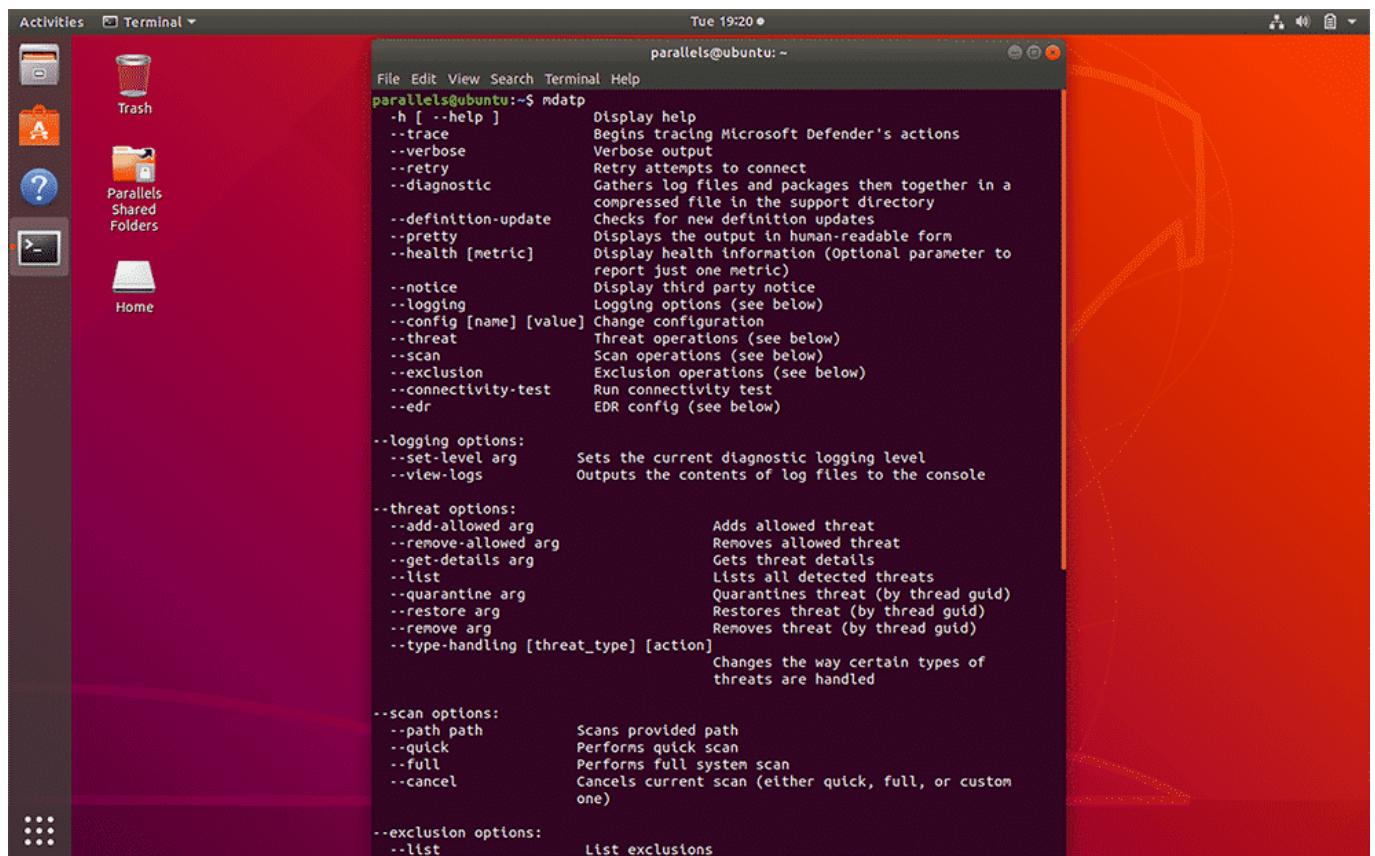
Antivirus : Microsoft étend Defender ATP à Linux et Android

L'antivirus de Microsoft couvre désormais les trois principales plates-formes *desktop*.

Lancé sur Windows en 2006, il était arrivé sur Mac à la mi-2019*. Le voilà maintenant [disponible sur les systèmes Linux](#). Ce en tant que composante de la suite de sécurité sur abonnement Microsoft Defender ATP.

Le déploiement se fait soit en ligne de commande, soit *via* des outils comme Puppet ou Ansible. Une licence Microsoft Defender ATP **for Servers** est nécessaire. La liste de compatibilité officielle comprend six OS :

- Red Hat Enterprise Linux (version 7.2 et ultérieures)
- CentOS (7.2+)
- Ubuntu 16.04 et les LTS suivantes
- SUSE Linux Enterprise Server (12+)
- Debian (9+)
- Oracle Linux (7.2+)



```
parallels@ubuntu: ~
File Edit View Search Terminal Help
parallels@ubuntu:~$ mdatp
-h [ --help ]           Display help
--trace                Begins tracing Microsoft Defender's actions
--verbose              Verbose output
--retry                Retry attempts to connect
--diagnostic           Gathers log files and packages them together in a
                       compressed file in the support directory
--definition-update    Checks for new definition updates
--pretty               Displays the output in human-readable form
--health [metric]      Display health information (optional parameter to
                       report just one metric)
--notice               Display third party notice
--logging              Logging options (see below)
--config [name] [value] Change configuration
--threat               Threat operations (see below)
--scan                 Scan operations (see below)
--exclusion             Exclusion operations (see below)
--connectivity-test    Run connectivity test
--edr                  EDR config (see below)

--logging options:
--set-level arg        Sets the current diagnostic logging level
--view-logs            Outputs the contents of log files to the console

--threat options:
--add-allowed arg      Adds allowed threat
--remove-allowed arg   Removes allowed threat
--get-details arg      Gets threat details
--list                 Lists all detected threats
--quarantine arg       Quarantines threat (by thread guid)
--restore arg          Restores threat (by thread guid)
--remove arg           Removes threat (by thread guid)
--type-handling [threat_type] [action]
                       Changes the way certain types of
                       threats are handled

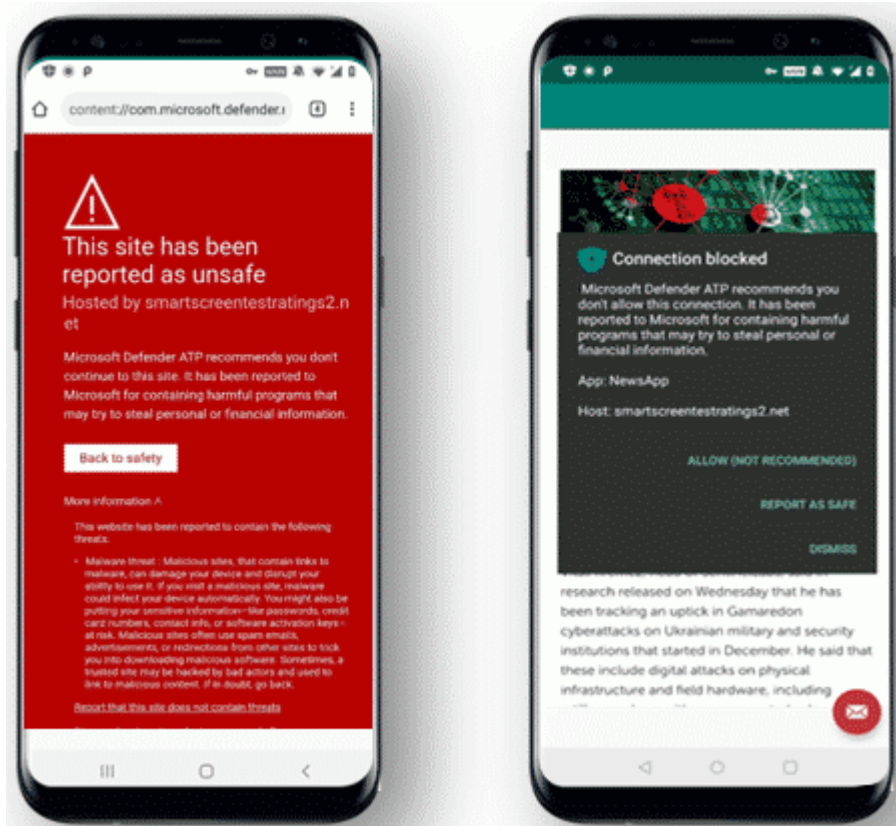
--scan options:
--path path            Scans provided path
--quick                Performs quick scan
--full                 Performs full system scan
--cancel               Cancels current scan (either quick, full, or custom
                       one)

--exclusion options:
--list                 List exclusions
```

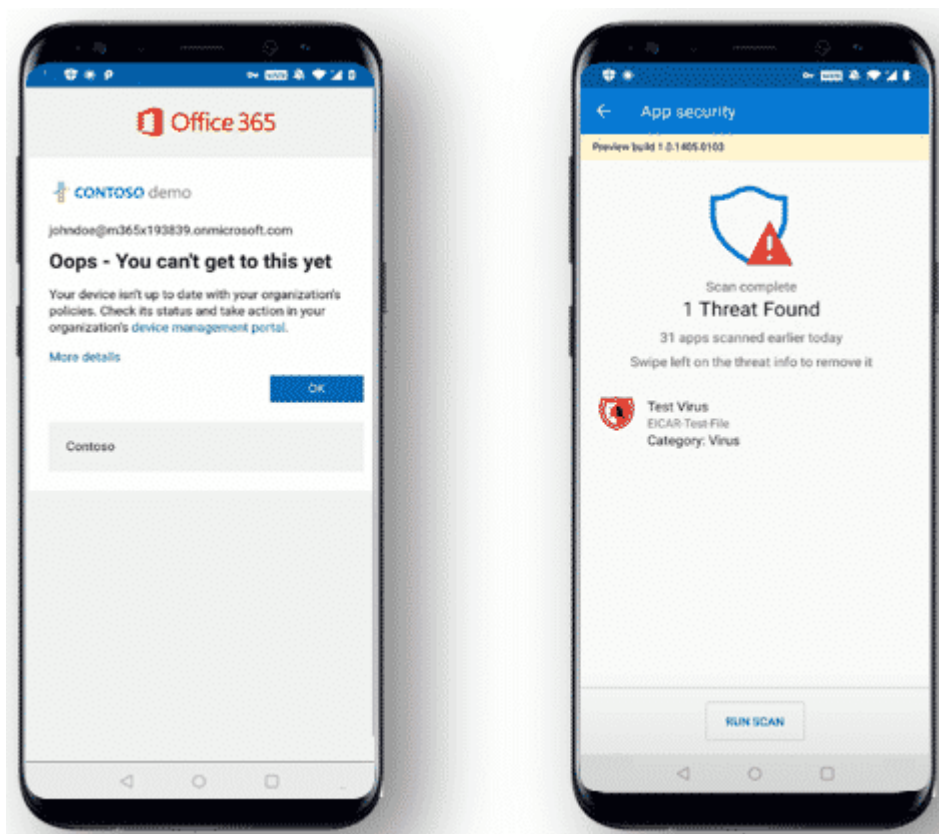
Android : Intune obligatoire

Parallèlement à la disponibilité générale sur Linux, Microsoft pousse une [préversion sur Android](#). Pour en avoir un aperçu, il faut activer les fonctionnalités expérimentales de Defender ATP. On accède alors à :

- Une protection web (*antiphishing* et blocage des connexions réseau indésirables, sur la base de la technologie SmartScreen)
- La détection des applications malveillantes (en complément à des outils comme Google Play Protect)
- Un contrôle d'accès aux données, sur la base de profils de risques attribués aux terminaux (en lien avec Endpoint Manager)



Le déploiement peut se faire aussi bien en mode administrateur d'Android que sur les appareils gérés avec Android Enterprise. Dans les deux cas, Intune est, en l'état, le seul MDM pris en charge.



Pas d'échéance annoncée pour la disponibilité générale. On aura cependant relever que, [sur Mac](#) comme sur Linux, le délai à partir de l'ouverture de la bêta publique été de deux à trois mois. Quant au lancement sur iOS, il interviendra « plus tard cette année ».

* À cette occasion, la marque « Microsoft Defender ATP » avait pris le relais de « Windows Defender ATP ».

Illustrations © Microsoft