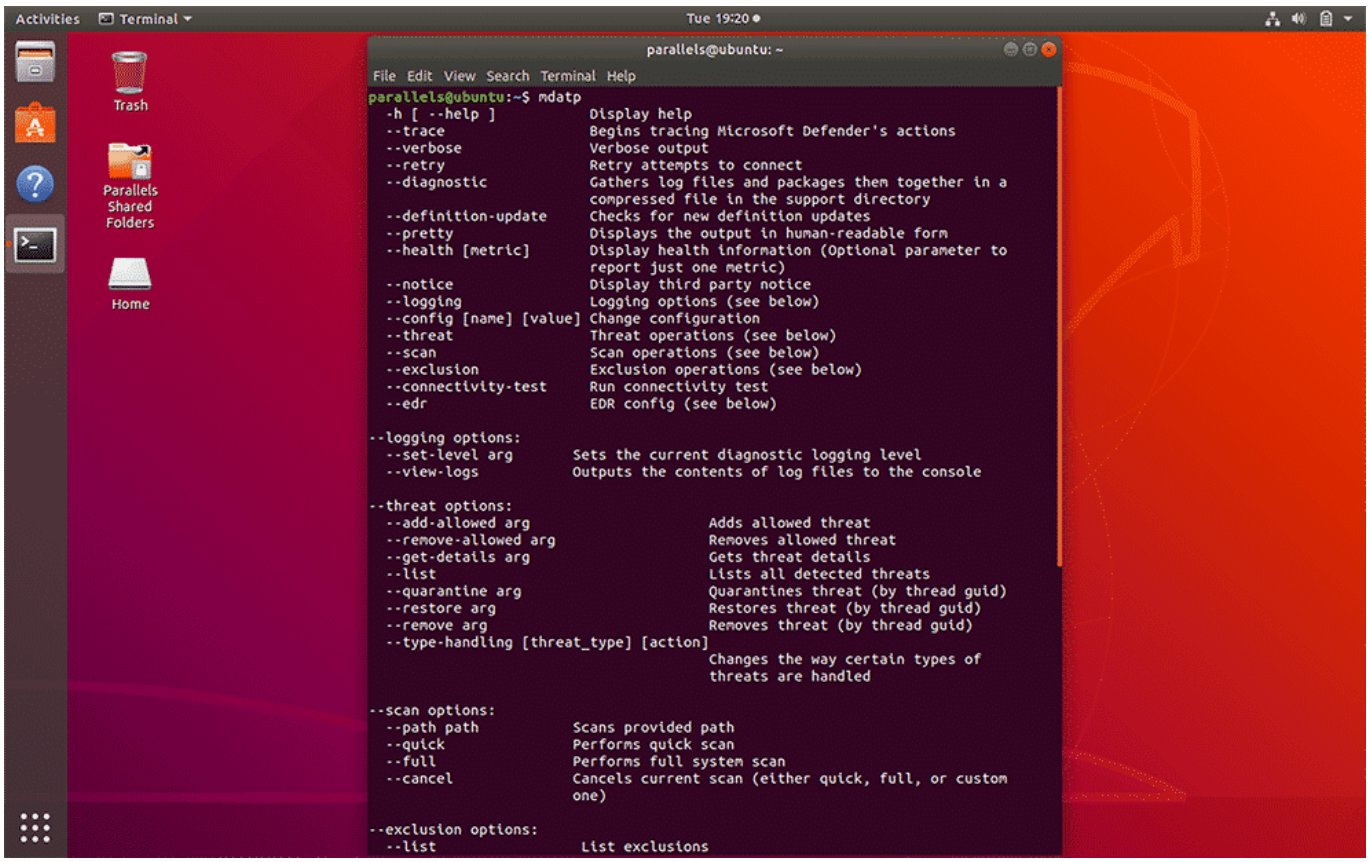
Antivirus : Microsoft étend Defender ATP à Linux et Android

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 :

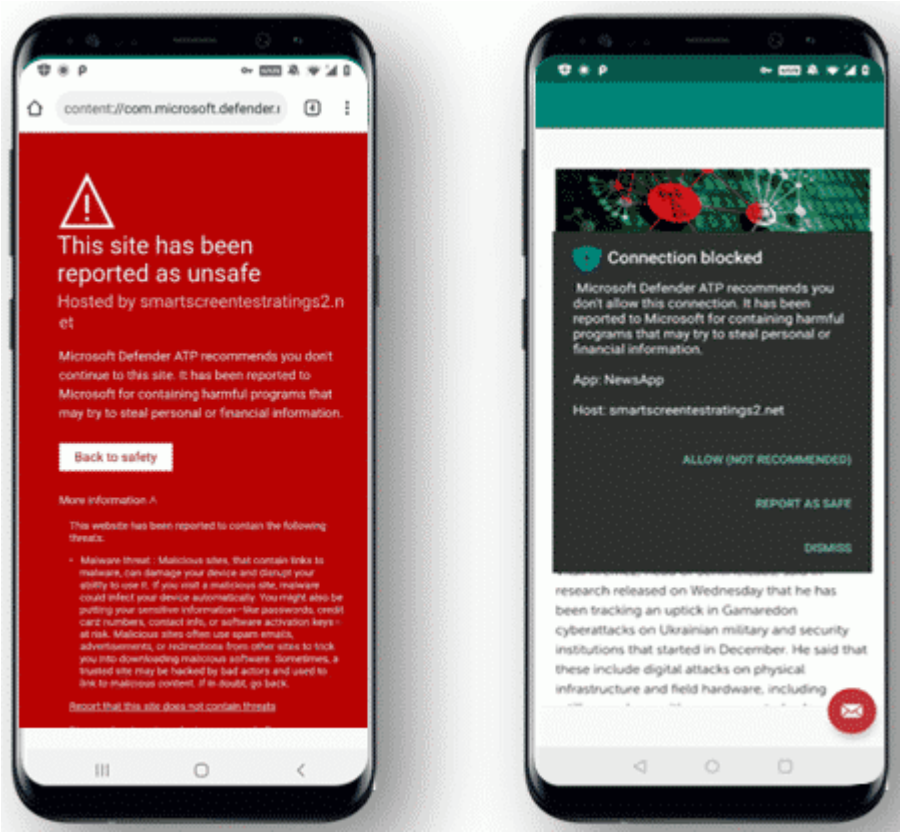
- Red Hat Enterprise Linux (version 7.2 et ultérieures)
- CentOS (7.2+)
- Ubuntu 16.04 et les LTS suivantes
- SUSE Linux Enterprise Server (12+)
- Debian (9+)
- Oracle Linux (7.2+)



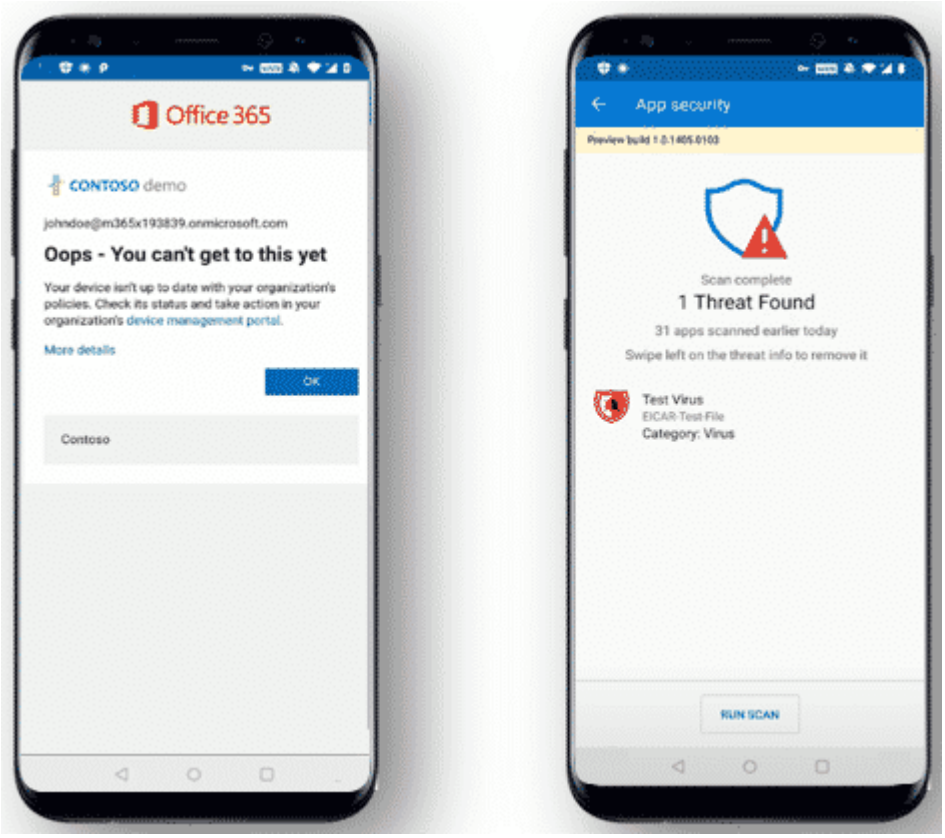
Android : Intune obligatoire

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