

Antivirus, EDR : bien protéger les postes de travail

L'antivirus de 2015 ne suffit plus. Comprendre ce qui protège réellement un parc en 2026.

10 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/antivirus-edr

Le poste de travail est là où tout commence : c'est lui qui ouvre les emails, les pièces jointes et les liens. Or l'antivirus traditionnel, qui compare les fichiers à une liste de menaces connues, laisse passer les attaques modernes, conçues pour être inédites à chaque envoi.

1. Antivirus classique et EDR : la différence

L'antivirus classique fonctionne par signatures : il reconnaît les fichiers malveillants déjà répertoriés. Efficace contre les menaces de masse, il est aveugle face à un malware fabriqué la veille.

L'EDR (Endpoint Detection & Response) observe les comportements : un processus Word qui lance PowerShell, un programme qui chiffre des centaines de fichiers en quelques secondes, une connexion sortante anormale. Il détecte l'attaque à sa manière d'agir, pas à son apparence — et permet d'isoler un poste à distance en cas d'alerte.

2. Ce qu'une protection de poste doit couvrir

- Analyse en temps réel des fichiers et des comportements
- Protection du navigateur et filtrage des sites malveillants
- Analyse des pièces jointes et des liens dans les emails
- Contrôle des périphériques USB
- Possibilité d'isoler un poste du réseau à distance
- Tableau de bord centralisé pour voir l'état de tout le parc

3. Les erreurs qui annulent la protection

- Des licences expirées sur une partie du parc (la protection s'arrête en silence)
- Des exclusions d'analyse trop larges ajoutées « pour que le logiciel métier fonctionne »
- Des alertes que personne ne lit : une détection sans réaction ne sert à rien
- Des utilisateurs administrateurs de leur poste, capables de désactiver la protection
- Croire que le Mac ou le smartphone « n'ont pas besoin d'antivirus »

4. L'outil ne suffit pas : la supervision

Un EDR génère des alertes qu'il faut savoir lire et traiter, y compris la nuit et le week-end — c'est précisément là que les attaquants agissent. Pour une TPE/PME sans équipe informatique dédiée, la bonne formule est souvent un EDR supervisé par un prestataire (service dit MDR) : l'outil détecte, des humains

qualifiés analysent et réagissent.

5. Choisir : les questions à poser

- Couverture : Windows, Mac, serveurs, et idéalement mobiles — un parc protégé aux trois quarts ne l'est pas
- Console centralisée : voir en un écran l'état de tout le parc, les postes en retard, les alertes en cours
- Capacité de réponse : isoler un poste à distance, tuer un processus, restaurer — pas seulement détecter
- Poids sur les machines : les solutions modernes sont légères, testez avant de déployer partout
- Offre de supervision (MDR) associée si vous n'avez pas d'équipe pour lire les alertes

BON À SAVOIR

Sous Windows, Microsoft Defender (intégré) atteint aujourd'hui un très bon niveau pour un poste isolé bien géré. Ce qui manque à une entreprise n'est pas tant le moteur que la gestion : console de parc, alertes centralisées, réponse à distance — ce que les offres professionnelles (Defender for Business inclus) apportent pour quelques euros par poste et par mois.

L'essentiel à retenir

- 01 Vérifier que chaque poste et serveur a une protection active et à jour
- 02 Privilégier un EDR à un antivirus par signatures seul
- 03 Centraliser les alertes et désigner qui les traite
- 04 Tester la procédure d'isolement d'un poste à distance
- 05 Retirer les droits administrateur des utilisateurs
- 06 Envisager une supervision externe (MDR) si personne ne peut réagir 24/7

Questions fréquentes

L'antivirus gratuit de Windows suffit-il ?

Pour un particulier soigneux, souvent oui. Pour une entreprise, le moteur n'est que la moitié du sujet : sans console centrale, vous ne savez pas si la protection est active partout, personne ne voit les alertes, et rien ne permet d'isoler un poste compromis à distance. C'est cette couche de gestion que vous achetez avec une offre professionnelle.

EDR, XDR, MDR... qui fait quoi ?

L'EDR surveille et protège les postes et serveurs (endpoints). Le XDR étend la surveillance à d'autres sources : messagerie, cloud, réseau. Le MDR n'est pas un logiciel mais un service : des analystes humains qui surveillent votre EDR/XDR 24/7 et réagissent à votre place. Pour une PME sans équipe sécurité, la combinaison EDR + MDR est généralement le bon rapport protection/budget.

Mon EDR génère des alertes en permanence, c'est normal ?

Un flot d'alertes non triées est le signe d'un réglage à revoir : trop de bruit fait rater la vraie alerte. Faites affiner la configuration (exclusions ciblées et documentées, sensibilité) par le prestataire, et exigez que chaque alerte restante ait un traitement défini : qui la lit, dans quel délai, avec quelle action.

Peut-on attraper un malware sans rien télécharger ?

C'est rare mais possible via des failles du navigateur ou des plugins (attaques dites « drive-by »), et surtout par les canaux qu'on oublie : clés USB, macros de documents Office, mises à jour piégées de logiciels piratés. D'où le trio : navigateur à jour, macros bloquées par défaut, et jamais de logiciels crackés dans l'entreprise.

Pour aller plus loin

Cybermalveillance.gouv.fr — protéger ses appareils — www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

ANSSI — Guide d'hygiène informatique — cyber.gouv.fr/publications/guide-dhygiene-informatique

Besoin d'aide pour le mettre en place ?

Audit, durcissement, accompagnement : Cyberionis sécurise les TPE, PME et collectivités, à Nancy, Lure et à distance.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr