



COMPARATIF DÉCISIONNEL

EDR ou antivirus : la fiche de choix pour votre PME

Utilisez cette fiche pour relier votre niveau d'exposition, vos ressources internes et vos besoins de supervision à la protection la plus cohérente. L'objectif n'est pas de choisir l'outil le plus complet, mais celui que votre PME pourra réellement administrer et exploiter.

Au sommaire

- 1 À retenir avant de choisir
- 2 Antivirus professionnel ou EDR : comparer les capacités
- 3 Méthode de décision en 5 étapes
- 4 Ma PME est-elle prête pour un EDR ?
- 5 Repère final

À retenir avant de choisir

Un antivirus professionnel bloque principalement les menaces connues et reste généralement plus simple à administrer.

L'EDR est particulièrement pertinent lorsque la PME doit mieux détecter les attaques discrètes, les rançongiciels ou les usages en télétravail.

La protection des postes doit être associée à des mises à jour, des sauvegardes testées, une authentification renforcée et une procédure de réponse aux incidents.

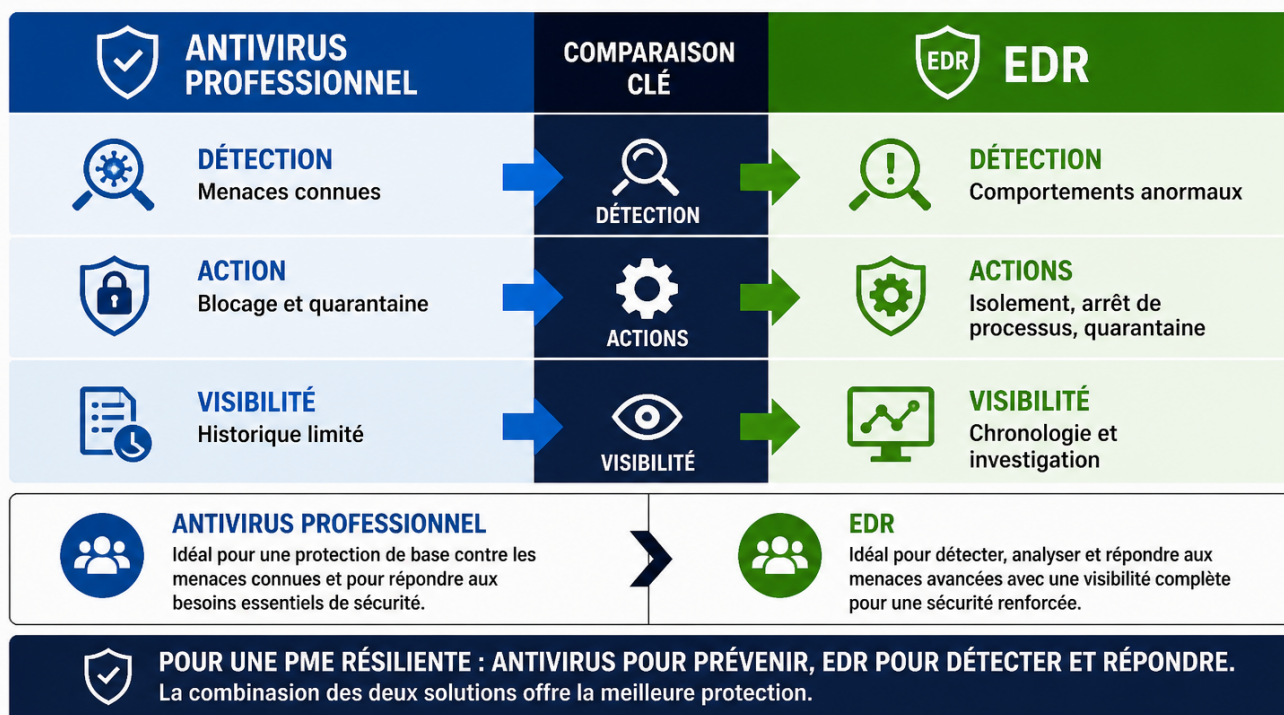
Un EDR observe les événements sur les terminaux, recherche des comportements suspects et facilite la réponse ainsi que l'investigation.

Une solution plus avancée n'est utile que si les alertes peuvent être analysées et traitées.

ANTIVIRUS PROFESSIONNEL vs EDR

QUELLE SOLUTION POUR PROTÉGER EFFICACEMENT VOTRE PME ?

Deux approches complémentaires, des niveaux de protection différents.
Comparez leurs capacités pour faire le bon choix pour votre entreprise.



INFOGRAPHIE Schéma en français comparant le fonctionnement d'un antivirus et d'un EDR pour une PME

Antivirus professionnel ou EDR : comparer les capacités

Critère	Antivirus professionnel	EDR
Objectif principal	Bloquer les fichiers malveillants, logiciels indésirables et menaces déjà identifiées.	Détecter des comportements suspects et aider à répondre à un incident.
Mode de détection	Signatures, règles, réputation des fichiers et analyses complémentaires selon l'offre.	Analyse des comportements et des séquences d'événements sur les terminaux.
Visibilité	Protection et administration centralisée des postes selon l'offre retenue.	Collecte d'événements et vision plus approfondie de ce qui s'est produit sur un poste.
Réponse	Blocage ou mise en quarantaine selon les fonctions proposées.	Peut faciliter l'isolation d'un poste, l'arrêt d'un processus ou la mise en quarantaine d'un fichier selon la solution.
Investigation	Plus limitée pour reconstituer une chaîne d'actions.	Aide à comprendre la chronologie et le contexte d'un comportement suspect.
Administration	Souvent plus accessible pour une petite équipe.	Demande davantage de compétences, de supervision et de temps de traitement des alertes.



ANTIVIRUS PROFESSIONNEL vs EDR

QUELLE SOLUTION POUR PROTÉGER EFFICACEMENT VOTRE PME ?

Les deux approches sont complémentaires.
Le choix dépend de vos risques, de vos ressources et de vos objectifs de sécurité.



CRITÈRES	ANTIVIRUS PROFESSIONNEL	EDR	VIGILANCE PME
1. MENACES CONNUES	Détection et blocage adaptés	Couverture généralement intégrée ou associée	Vérifier le périmètre exact de l'offre
2. COMPORTEMENTS ANORMAUX	Analyse variable selon la solution	Fonction centrale de la plateforme	Configurer correctement les règles
3. INVESTIGATION	Historique souvent limité	Chronologie détaillée des événements	Rétention des données variable
4. RÉPONSE À INCIDENT	Blocage ou quarantaine principalement	Isolément, arrêt de processus et actions à distance selon l'offre	Validation humaine nécessaire
5. ADMINISTRATION	Plus simple pour une petite équipe	Plus riche, donc plus exigeante	Prévoir du temps ou une supervision externalisée

NOTRE RECOMMANDATION POUR UNE PME

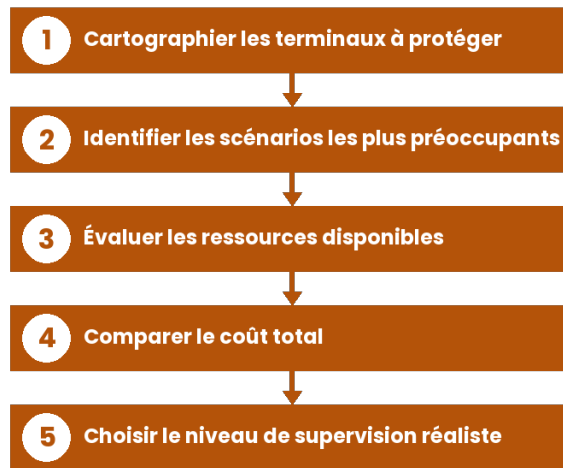
Un antivirus professionnel est indispensable pour bloquer les menaces connues. L'EDR apporte visibilité, contexte et capacité d'action face aux attaques complexes.

LES BÉNÉFICES POUR VOTRE PME

- Meilleure protection globale
- Visibilité et maîtrise accrues
- Réduction du temps de détection et de réponse
- Continuité d'activité renforcée
- Valorisation de vos données et de vos ressources

COMPARATIF Les capacités à mettre en regard avant de choisir entre antivirus professionnel et EDR.

Méthode de décision en 5 étapes



1 **Cartographier les terminaux à protéger**

Recensez les postes, serveurs et équipements mobiles concernés, ainsi que les situations de télétravail ou d'utilisation hors du réseau habituel.

2 **Identifier les scénarios les plus préoccupants**

Demandez-vous si votre priorité est de bloquer les menaces connues ou de mieux repérer des comportements anormaux, notamment face aux rançongiciels et aux attaques sans fichier.

3 **Évaluer les ressources disponibles**

Vérifiez qui installera la solution, suivra les alertes, analysera les faux positifs et décidera des mesures à prendre en cas d'incident.

4 **Comparer le coût total**

Ne comparez pas uniquement le tarif par terminal : prenez aussi en compte la licence, le déploiement, la supervision et le temps consacré au traitement des alertes.

5 **Choisir le niveau de supervision réaliste**

Si votre équipe ne peut pas traiter les alertes d'un EDR, étudiez une offre EDR managée ou retenez une protection plus simple à administrer.

Ma PME est-elle prête pour un EDR ?

☐

Nous avons identifié les postes, serveurs et équipements mobiles à couvrir.

Incluez les terminaux utilisés en télétravail.

☐

Nous savons qui recevra et traitera les alertes.

Une alerte non suivie réduit l'intérêt de la solution.

☐

Nous pouvons analyser les comportements inhabituels.

L'EDR fournit du contexte qui doit être interprété.

☐

Nous avons défini une procédure de réponse aux incidents.

Précisez les actions à engager lorsqu'un poste est suspect.

☐

Nous avons prévu le temps de gestion des faux positifs.

Intégrez ce temps dans l'évaluation du coût total.

☐

Nous envisageons une supervision managée si les compétences internes sont limitées.

L'accompagnement peut être préférable à un EDR laissé sans suivi.

! Ne pas confondre outil et protection complète

Un antivirus ou un EDR ne remplace pas les autres mesures de sécurité. Vérifiez également les mises à jour, les sauvegardes testées, l'authentification renforcée et la procédure de réponse aux incidents.

Repère final

Privilégiez un antivirus professionnel si votre besoin principal est de sécuriser des postes standards avec une administration accessible et peu d'alertes complexes. Orientez-vous vers un EDR si vous recherchez une visibilité plus approfondie, une détection comportementale et une capacité de réponse accrue, avec les ressources nécessaires pour exploiter ses alertes.

Le choix dépend de l'exposition aux menaces, du nombre de postes, des compétences disponibles et du niveau de supervision recherché. Évaluez la solution dans le contexte réel de votre PME.