

Antivirus vs outil de détection et de correction des menaces sur les terminaux :

TABLEAU COMPARATIF

Les cybermenaces ne cessent d'augmenter. La sécurité multicouche représente assurément la meilleure arme pour protéger les réseaux et les utilisateurs finaux contre les menaces actuelles et futures.

Elle propose deux types de protection pour les utilisateurs finaux : **antivirus classique et outil de détection et de correction des menaces sur les terminaux (EDR)**. Les deux offrent des avantages aux MSP, mais à différents niveaux. L'un ne remplace pas l'autre, chacun étant conçu pour traiter des problèmes spécifiques.

Lorsque vous devez faire un choix entre les deux, il est important de prendre en compte plusieurs facteurs, tels que le type d'entreprise et d'utilisateurs ayant besoin d'une protection, ainsi que le coût de chaque solution. N-able propose les deux solutions afin que vous puissiez fournir le meilleur niveau de service à vos clients.

	ANTIVIRUS	EDR
Données contextuelles et enquête sur les menaces	Limitées	Complètes
Options d'élimination, de mise en quarantaine, de correction et de restauration	Élimination/mise en quarantaine uniquement	Toutes
Utilisation du système CVE (vulnérabilités et expositions communes)	Non	Oui
Protection des utilisateurs hors ligne	Nécessite des définitions à jour	Oui
Stratégie pour autoriser/bloquer les périphériques USB par fournisseur/type/série/produit	Non	Oui
Stratégie de déconnexion du réseau pour contenir les menaces	Non	Oui
Stratégie de contrôle des paramètres du pare-feu sur les points de terminaison	Non	Oui
Empêche et détecte un plus large éventail de menaces quasiment en temps réel	Non	Oui
Utilisation des ressources	Modérée	Faible
Bloque les menaces de type « packers » (comportement anodin)	Non	Oui
Bloque les menaces de type « wrapper/polymorphes/dissimulées »	Nécessite des définitions à jour	Oui
Bloque les attaques sans fichiers	Non	Oui
Bloque les menaces inconnues (zero-day)	Nécessite des définitions à jour	Oui
Détection basée sur les signatures	Oui	Oui
Coût	Faible	Modéré
Profil de risque de l'utilisateur	Faible	Élevé

[Testez la différence avec N-able EDR !](#)