Caractéristiques	CyberDomme-AI	Solutions traditionnelles	Solutions basées sur le cloud	Système de sécurité Endpoint
Souveraineté des données	Déploiement locale possible pour garantir la souveraineté	Souvent dépend des lois sur la protection des données	Peut être un problème selon l'emplacement des serveurs	Dépend de la gestion des données locales
Coûts d'entretiens	Économies sur les coûts énergétiques et de cybersécurité	Souvent élevé, avec de coûts cachés	Coût variable selon le modèle d'abonnement	Coûts d'entretien pour les mises à jour et la gestion
Détection des menaces	Approche biométrique, apprentissage fédéré	Basée sur des signatures statiques	Détection basée sur des modèles de comportement	Détection sur l'appareil souvent limité
Réaction en temps réel	Réaction immédiate aux intrusions	Réaction souvent tardive	Réaction rapide, mais dépende la latence du réseau	Peut être instantanée, mais limité a l'appareil
Résilience aux cyberattaques	Résilience adaptive avec apprentissage de chaque incident	Limitée par la capacité de mise à jour	Souvent robuste, mais dépend de la sécurité du fournisseur	Dépend de la configuration et des mises à jour
Évolutivité	Conçu pour évoluer avec les menaces	Souvent rigide et difficile à adapter	Évolutif, mais dépend des limitations du fournisseur	Peut nécessiter des mises a jour fréquentes
Protection des données	Chiffrement de bout en bout, journalisation	Chiffrement disponible mais varie selon les solutions	Chiffrement dépend du fournisseur, peut ne pas être uniforme	Chiffrement local souvent limité