

Services de sécurité et de résilience de l'IA

Faites confiance à votre utilisation de l'IA



Relever les défis liés à l'adoption de l'IA

L'intelligence artificielle (IA) est une révolution pour les entreprises, car elle favorise l'innovation et accélère la prise de décisions. Mais un potentiel aussi vaste amène forcément son lot de difficultés. L'adoption de l'IA génère de vives inquiétudes en matière de sécurité, de confiance et de conformité, et soumet les organisations à de nouvelles contraintes. Chez Dell Technologies, nous avons complètement repensé le fonctionnement de la sécurité de l'IA. Notre approche hors du commun intègre la gestion des données, la sécurité de l'infrastructure et la protection des modèles d'IA pour vous proposer une solution complète et personnalisée. Que vous n'en soyez qu'à vos premiers pas ou que vous souhaitiez étendre vos solutions existantes, nos services complets sont conçus pour adopter l'IA plus rapidement, mais aussi de manière plus fiable et sécurisée.

L'IT n'est pas seul responsable de la sécurité

La sécurité moderne de l'IA appelle la collaboration entre les équipes. C'est un sport collectif : toute l'entreprise doit contribuer aux conversations et aux décisions. Les modèles traditionnels IT cloisonnés ne sont plus d'actualité dans un monde qui évolue sans cesse. Notre approche unique regroupe les données, l'infrastructure, les applications et les modèles dans une seule stratégie uniformisée, qui s'adapte aux besoins spécifiques de votre entreprise et qui offre une solution complète capable de vous propulser en tête de course.

Relever les défis de sécurité uniques de l'IA

L'adoption de l'IA pose de nouvelles questions complexes, en lien avec la sécurité et la conformité, qui peuvent nuire aux avantages promis par cette technologie, notamment :

- Violations de données et perte de propriété intellectuelle (PI) en raison d'une protection inadéquate des données ou d'un accès non autorisé.
- Menaces augmentées par l'IA, comme les attaques conçues pour tromper les systèmes d'IA, la manipulation des modèles ou la corruption des données d'entraînement.
- Défis liés à la disponibilité des outils IA désormais stratégiques, tels que les agents de support, censés rester opérationnels en continu.
- Failles de sécurité de la chaîne logistique tierce issues de systèmes interconnectés.
- Surface d'attaque en expansion à mesure que les applications d'IA évoluent dans les environnements hybrides et multicloud.
- Bien qu'elles ne soient pas un problème de sécurité à l'origine, les hallucinations peuvent induire les utilisateurs en erreur.

Principaux avantages

Confiance et transparence renforcées

protégez les données, la propriété intellectuelle et l'intégrité de l'IA pour entretenir la confiance des parties prenantes.

Résilience opérationnelle

assurez-vous que vos systèmes d'IA stratégiques restent opérationnels et à l'épreuve des menaces.

Conformité aux réglementations

respectez les réglementations de votre secteur et de votre gouvernement afin d'éviter des pénalités coûteuses et la fragilisation de votre réputation.

Solutions évolutives

mettez en œuvre des mesures de sécurité de l'IA adaptatives qui évoluent avec votre organisation et son infrastructure technologique.

Conseils et assistance d'experts

collaborez avec des experts en sécurité compétents pour personnaliser votre solution et générer des résultats mesurables.

Des services de bout en bout pour fournir une architecture de sécurité sur mesure

Notre architecture de sécurité développée par Dell est pensée pour répondre à vos besoins uniques et jeter les bases flexibles et fiables de votre infrastructure. Elle s'intègre parfaitement à Dell AI Factory, applique les principes Zero-Trust et prend en charge les technologies partenaires intégrées d'une main experte pour favoriser l'innovation avant-gardiste en toute sécurité.



Modèles et applications d'IA



Données



Infrastructure

	Fonctionnalités
Conseils Aligner la sécurité de l'IA sur les besoins de votre organisation et les exigences de conformité	<ul style="list-style-type: none">Les services de conseils pour la sécurité et la résilience de l'IA comprennent des ateliers commerciaux et techniques visant à élaborer une stratégie complète de sécurité et de disponibilitéCISO Advisor pour l'IA fournit un CISO virtuel expert en IA pour déployer votre stratégie de sécurité IALa sécurité des données pour l'IA aide à limiter les menaces et les risques de sécurité des données
Implémentation Concevoir et implémenter des logiciels de sécurité pour augmenter la visibilité de la pile d'IA	<ul style="list-style-type: none">La conception et la configuration des logiciels de sécurité intègrent les outils qui protègent la gestion des accès, les applications et les réseaux
Gérer Bénéficiez d'une excellente visibilité sur l'ensemble de la pile pour détecter les menaces et réagir rapidement	<ul style="list-style-type: none">La MDR (Managed Detection and Response) détecte les menaces 24 h/24, 7 j/7 sur l'ensemble des données, de l'infrastructure, des applications et des modèlesLe pare-feu d'IA géré met en place un ensemble isolé de garde-corps basés sur l'IA et analyse les prompts et les résultats pour vérifier la conformité aux politiquesLes tests de pénétration pour l'IA simulent les attaques conçues pour tromper les systèmes d'IA et mettent au jour les points faiblesLes services de réponse aux incidents et de récupération vous aident à récupérer rapidement et à reprendre vos activités avec un minimum d'interruptions

Forgez un avenir IA sécurisé en toute confiance

Les services de sécurité et de résilience de l'IA de Dell sont conçus pour répondre aux nouveaux risques associés à l'adoption de l'IA au sein de votre organisation. Par défaut, nos services collaborent avec vos équipes pour intégrer l'IA le plus rapidement possible. Notre expertise vous oriente tout au long dans la planification stratégique, de la mise en œuvre des solutions et des services de sécurité gérés afin de réduire les charges opérationnelles et de favoriser l'innovation sécurisée avec l'IA.



Découvrir les [services de sécurité et de résilience](#) de Dell



[Contacter](#) un expert Dell Technologies



Participez à la conversation avec #DellTechnologies