

Services voor AI-beveiliging en -veerkracht

Vertrouw op uw gebruik van AI



De uitdagingen van AI-adoptie aanpakken

Kunstmatige intelligentie (AI) is een doorbraak voor bedrijven, die baanbrekende innovatie en snellere besluitvorming mogelijk maakt. Maar een groot potentieel brengt ook aanzienlijke uitdagingen met zich mee. Bij AI-adoptie ontstaan unieke zorgen over beveiliging, vertrouwen en naleving, waardoor organisaties onder nieuwe druk komen te staan. Bij Dell Technologies hebben we de manier waarop AI-beveiliging moet werken opnieuw vorm gegeven. Onze aanpak integreert databeheer, infrastructuurbeveiliging en AI-modelbescherming op unieke wijze om een uitgebreide, op maat gemaakte oplossing te bieden. Of u nu een beginner bent op het gebied van AI of bestaande oplossingen wilt schalen, onze end-to-end services zijn ontworpen om AI-adoptie sneller, veiliger en betrouwbaarder te maken.

Beveiliging is niet alleen de taak van IT

Moderne AI-gerelateerde beveiliging vereist samenwerking tussen teams. AI-beveiliging is een teamsport die input en besluitvorming vanuit uw hele organisatie vereist. Traditionele IT-bedrijfsmodellen in silo's werken niet in dit veranderende landschap. Onze unieke aanpak brengt data, infrastructuur, applicaties en modellen samen in één samenhangende strategie die zich aanpast aan uw specifieke bedrijfsbehoeften en een holistische oplossing biedt waarmee u voorop kunt blijven lopen.

De unieke beveiligingsuitdagingen van AI aanpakken

AI-adoptie introduceert complexe beveiligings- en nalevingsoverwegingen die de potentiële voordelen in gevaar kunnen brengen, zoals:

- Datalekken en verlies van intellectueel eigendom (IP) als gevolg van onvoldoende databescherming of onbevoegde toegang.
- AI-gestuurde bedreigingen zoals vijandige aanvallen, modelmanipulatie of vergiftiging van trainingsdata.
- Beschikbaarheidsuitdagingen voor nu kritieke AI-tools, zoals ondersteuningsmedewerkers, om continu operationeel te zijn.
- Kwetsbaarheden in de leveringsketen van derden die het gevolg zijn van onderling verbonden systemen.
- Steeds uitgebreidere aanvalsoppervlakken naarmate AI-applicaties worden geschaald in hybride en multicloudomgevingen.
- Hoewel hallucinaties niet louter een veiligheidsprobleem zijn, kunnen ze gebruikers misleiden

Belangrijkste voordelen

Verbeterd vertrouwen en transparantie: bescherm data, intellectueel eigendom en AI-integriteit om het vertrouwen onder belanghebbenden te behouden.

Operationele veerkracht: houd uw bedrijfskritieke AI-systemen operationeel en bestand tegen bedreigingen.

Naleving van regelgeving: help te voldoen aan de regelgeving van uw branche en overheid om dure boetes en reputatieschade te voorkomen.

Schaalbare oplossingen: implementeer aanpasbare AI-beveiligingsmaatregelen die meegroeien met uw organisatie en haar technologiystack.

Deskundige support en begeleiding: werk samen met bewezen beveiligingsexperts om uw oplossing op maat te maken en meetbare resultaten te leveren.

End-to-end services om een op maat gemaakte beveiligingsarchitectuur te leveren

De door Dell ontwikkelde beveiligingsarchitectuur is ontworpen om aan uw unieke behoeften te voldoen en biedt een flexibele en betrouwbare basis. De architectuur integreert naadloos met de Dell AI Factory, maakt gebruik van zero trust-principes en bevat vakkundig geïntegreerde partnertechnologieën om veilige, vooruitstrevende innovatie te stimuleren.

	Functies
AI-modellen en -applicaties	
Data	
Infrastructuur	
Advies Stem uw AI-beveiliging af op de behoeften en nalevingsvereisten van de organisatie	• Beveiliging en veerkracht voor AI Advisory Services omvatten zakelijke en technische workshops om een uitgebreide beveiligings- en beschikbaarheidsstrategie te ontwikkelen • CISO-adviseur voor AI biedt een virtuele CISO die een expert is in AI om uw AI-beveiligingsstrategie een boost te geven • Databeveiliging voor AI helpt bedreigingen voor databeveiliging en risico's voor uw data te verminderen
Implementatie Ontwerp en implementeer beveiligingssoftware om de zichtbaarheid van de AI-stack te vergroten	• Ontwerp en configuratie van beveiligingssoftware om tools te integreren die toegangsbeheer, applicaties en netwerken beschermen
Beheren Maak diepgaande zichtbaarheid in de stack mogelijk om snel bedreigingen te detecteren en erop te reageren	• Beheerde detectie en reactie (MDR) voor 24/7 detectie van bedreigingen in data, infrastructuur, applicaties en modellen • Beheerde AI-firewall legt een geïsoleerde reeks op AI gebaseerde beschermingsmaatregelen op en inspecteert prompts en outputs op naleving van beleid • Penetratietesten voor AI om vijandige aanvallen te simuleren en zwakke punten te ontdekken • Services voor incidentrespons en -herstel zodat u snel kunt herstellen en met minimale onderbreking weer aan de slag kunt gaan

Bouw met vertrouwen een veilige AI-toekomst

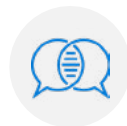
Dell heeft de AI-beveiligings- en veerkrachtservices ontworpen om nieuwe risico's aan te pakken die gepaard gaan met de integratie van AI in uw organisatie. Onze services zijn ontworpen om samen te werken met uw teams terwijl u AI zo snel mogelijk integreert. Ze bieden expertise om u te begeleiden bij strategische planning, implementatie van oplossingen en beheerde beveiligingsservices om de operationele lasten te verlichten, zodat u veilig kunt innoveren met AI.



Ontdek Dell [Security and Resiliency Services](#)



[Neem contact op](#) met een Dell Technologies expert



Neem deel aan het gesprek via [#DellTechnologies](#)