

Tjänster för AI-säkerhet och motståndskraft

Lita på hur du använder AI



Hantera utmaningarna med AI-implementering

Artificiell intelligens (AI) är avgörande för företag och möjliggör banbrytande innovation och snabbare beslutsfattande. Men de stora möjligheterna kommer även med betydande utmaningar. Med AI-implementering uppstår unika problem inom säkerhet, tillit och överensstämmelse, vilket ställer nya krav på organisationer. På Dell Technologies har vi omdefinierat hur AI-säkerhet ska fungera. Vår metod integrerar datahantering, infrastrukturens säkerhet och skydd av AI-modeller på ett unikt sätt och erbjuder en omfattande, skräddarsydd lösning. Oavsett om du är ny inom AI eller skalar befintliga lösningar är våra heltäckande tjänster utformade för att göra AI-implementeringen snabbare, säkrare och mer tillförlitlig.

Säkerhet är inte bara IT-avdelningens jobb

Modern AI-relaterad säkerhet kräver att alla team samarbetar med varandra. AI-säkerhet är en lagsport som kräver att hela organisationen deltar och fattar beslut. Traditionella silobaserade IT-driftsmodeller fungerar inte i detta föränderliga landskap. Vår unika metod införlivar data, infrastruktur, program och modeller i en enda sammanhängande strategi som anpassar sig efter dina specifika affärsbehov och erbjuder en helhetslösning som hjälper dig att ligga steget före.

Hantera AI:s unika säkerhetsutmaningar

AI-implementering introducerar komplexa säkerhets- och överensstämmelseöverväganden som kan äventyra dess potentiella fördelar, till exempel:

- Dataläckor och förlust av immateriell egendom (IP) på grund av otillräckligt dataskydd eller obehörig åtkomst.
- AI-drivna hot som attacker, modellmanipulation eller förgiftade träningsdata.
- Utmaningar med tillgänglighet för AI-verktyg som är kritiska här och nu, t.ex. supportagenter, för att kunna vara i drift kontinuerligt.
- Sårbarheter i leverantörskedjan från tredje part, som härrör från sammankopplade system.
- Utökade attackytor när AI-program skalas över hybrid- och flermolnsmiljöer.
- Även om det egentligen inte är ett säkerhetsproblem, men hallucinationer kan missleda användare

Viktiga fördelar

Förbättrat förtroende och transparens: Skydda data, immateriell egendom och AI-integritet för att bibehålla intressenternas förtroende.

Drifttålighet: Håll dina verksamhetskritiska AI-system i drift och motståndskraftiga mot hot.

Regelefterlevnad: Hjälpa till att uppfylla bransch- och myndighetsföreskrifter för att undvika kostsamma påföljder och förlorat anseende.

Skalbara lösningar: Driftsätt anpassningsbara AI-säkerhetsåtgärder som växer i takt med din organisation och dess teknikstack.

Expertsupport och rådgivning: Arbeta med beprövade säkerhetsexperten för att skräddarsy din lösning och leverera mätbara resultat.

Heltäckande tjänster för att leverera en skräddarsydd säkerhetsarkitektur

Vår Dell-utvecklade säkerhetsarkitektur är utformad för att uppfylla dina unika behov, vilket ger en flexibel och tillförlitlig grund. Den integreras sömlöst med Dell AI Factory, aktiverar nollförtroendepprinciper och införlivar expertintegrerad partnerteknik för att driva säker, framåtblickande innovation.

	Funktioner
AI-modeller och -program Råd Anpassa din AI-säkerhet efter organisationens behov och krav på regelefterlevnad	Säkerhet och motståndskraft för AI-rådgivningstjänster inkluderar verksamhetsinriktade och tekniska workshops för att utveckla en omfattande strategi för säkerhet och tillgänglighet CISO Advisor för AI tillhandahåller en virtuell CISO som är expert på AI för att köra igång din AI-säkerhetsstrategi Datasäkerhet för AI bidrar till att minska att dina data utsätts för säkerhetshot och risker
Data Implementera Utforma och implementera säkerhetsmjukvara för att öka AI-stackens synlighet	Utformning och konfiguration av säkerhetsprogram för att integrera verktyg som skyddar åtkomsthantering, program och nätverk
Infrastruktur Hantera Möjliggör ett synlighetsdjup över stacken för att snabbt upptäcka och reagera på hot	MDR (Managed Detection and Response) för hotdetektering dygnet runt av data, infrastruktur, program och modeller Hanterad AI-brandvägg visar upp en isolerad uppsättning AI-baserade skyddsräcken och granskar prompter och utdata så de följer aktuella policyer Intrångstest för AI för att simulera attacker och upptäcka svagheter Incident Response and Recovery Services hjälper dig att snabbt återställa och komma igång med verksamheten igen med minimala störningar

Skapa en säker AI-framtid med tillförsikt

Dells tjänster för AI-säkerhet och motståndskraft är utformade för att hantera nya risker som är förknippade med att AI integreras i organisationen. Våra tjänster är byggda för att fungera tillsammans med dina team så snabbt som möjligt när du använder AI och tillhandahåller expertis för att vägleda i strategisk planering, implementering av lösningar och hanterade säkerhetstjänster för att underlätta driftsbördan så att du kan förnya på ett säkert sätt med AI.



Utforska Dells [lösningar för säkerhet och motståndskraft](#)



[Kontakta](#) en Dell Technologies-expert



Var med i samtalet med [#DellTechnologies](#)