DELL Technologies

AIのセキュリティとレジリエンスに関するサービス

信頼をもってAIを使う

AI導入の課題への対処

人工知能(AI)は企業にとってのゲーム チェンジャーであり、画期的なイノベーションを実現し、意思決定を迅速化させます。ただし、大きな可能性を秘めている一方で、大きな課題も抱えています。AIの導入により、セキュリティ、信頼性、コンプライアンスにAI固有の懸念が生じ、企業に新たなプレッシャーがもたらされます。デル・テクノロジーズでは、AIセキュリティの仕組みを刷新しました。DELLのアプローチでは、データ管理、インフラストラクチャ セキュリティ、AIモデル保護を独自に統合し、包括的でカスタマイズされたソリューションを提供しています。AIを初めて使用する場合でも、既存のソリューションを拡張する場合でも、DELLのエンドツーエンドのサービスは、AIをより迅速かつ安全に、高い信頼性で導入できるように設計されています。

セキュリティはIT部門だけの仕事ではない

最新のAI関連のセキュリティには、複数のチームで協働する必要があります。AIセキュリティはチーム スポーツであり、組織全体からの意見と意思決定を必要とします。現在の変化し続ける状況においては、従来のサイロ化されたIT運用モデルは機能しません。DELL固有の手法は、データ、インフラストラクチャ、アプリケーション、モデルを単一の一貫した戦略に統合し、お客様の具体的なビジネス ニーズに合わせて調整して、お客様が常に先を行くために役立つ総合的なソリューションを提供します。

AI固有のセキュリティ課題に対処

AIを導入すると、次のようなセキュリティとコンプライアンスに関する複雑な考慮事項が生じ、潜在的なメリットが損なわれる可能性があります。

- 不十分なデータ保護や不正アクセスによるデータ侵害や知的財産(IP)の損失
- 敵対的攻撃、モデル操作、トレーニング データ ポイズニングなどのAIを活用した脅威
- サポート エージェントなど、現在重要なAIツールを継続的に運用するための可用性の課題
- 相互接続されたシステムに起因するサードパーティのサプライ チェーンの脆弱性
- AIアプリケーションのハイブリッド環境とマルチクラウド環境全体への拡張に伴う、攻撃対象領域の拡大
- 純粋にはセキュリティ上の懸念ではないものの、ユーザーをミスリードする可能性のあるハルシネーション

主なメリット

信頼性と透明性の向上：データ、知的財産、AIの整合性を保護し、ステークホルダー間の信頼を維持します。

オペレーショナル レジリエンス：ミッションクリティカルなAIシステムの運用を維持し、脅威に対する耐性を維持します。

法令遵守：業界および政府の規制を満たすことで、高額な罰則や評判の低下を回避します。

拡張性に優れたソリューション：組織とそのテクノロジー スタックに合わせて拡張できる適応性の高いAIセキュリティ対策を導入します。

エキスパートによるサポートとガイダンス：実績のあるセキュリティ エキスパートと協力して、ソリューションをカスタマイズし、測定可能な成果を実現します。

カスタマイズされたセキュリティ アーキテクチャを提供するエンドツーエンドのサービス

Dellが開発したセキュリティ アーキテクチャは、お客様固有のニーズを満たすように設計されており、柔軟で信頼性の高い基盤を提供します。Dell AI Factoryとシームレスに統合し、ゼロトラストの原則を推進し、専門的に統合されたパートナー テクノロジーを組み込んで、安全で先進的なイノベーションを推進します。

AIモデルと用途

データ

インフラストラクチャ

	機能
アドバイス 組織のニーズやコンプライアンス要件に合わせたAIセキュリティの調整	• **AIアドバイザリー サービスのセキュリティとレジリエンス**には、包括的なセキュリティと可用性戦略を策定するためのビジネス ワークショップと技術ワークショップが含まれる • **AI向けのCISOアドバイザー**は、AIのエキスパートである仮想CISOを提供し、AIセキュリティ戦略を開始する • **AI向けのデータ セキュリティ**で、データ セキュリティの脅威とデータに対するリスクを軽減する
実装 AIスタックの可視性を高めるセキュリティ ソフトウェアを設計および実装	• **セキュリティ ソフトウェアの設計と構成**で、アクセス管理、アプリケーション、ネットワークを保護するツールを統合する
管理 スタック全体を詳細に可視化し、脅威を迅速に検出して対応	• **Managed Detection and Response (MDR)**で、データ、インフラストラクチャ、アプリケーション、モデルにわたって24時間365日体制で脅威を検出する • **Managed AI Firewall**で、分離された一連のAIベースのガードレールをインポートし、ポリシーのコンプライアンスのプロンプトと出力を検査する • **Penetration Testing for AI**による敵対的攻撃のシミュレーションを行い、弱点を見出す • **Incident Response and Recovery Services**で、中断を最小限に抑えて迅速に復旧し、業務を再開する

安全なAIの未来を確実に構築

DellのAIセキュリティおよびレジリエンス サービスは、AIの組織への統合に関連する新たなリスクに対処するように設計されています。Dellのサービスは、お客様のチームと連携して、AIをできる限り迅速にオンボーディングできるように構築されており、戦略計画、ソリューションの実装、マネージド セキュリティ サービスをガイドする専門知識を提供し、運用上の負担を軽減して、AIを活用して安全にイノベーションを実現します。

Dellのセキュリティおよびレジリエンス サービスを詳しく見る

デル・テクノロジーズのエキスパートに問い合わせる

#DellTechnologiesで会話に参加する

DELL Technologies