DELL Technologies

KI-Services für Sicherheit und Resilienz

Vertrauen in die Nutzung von KI

Bewältigung der Herausforderungen der KI-Einführung

Künstliche Intelligenz (KI) ist ein Gamechanger für Unternehmen, denn sie ermöglicht bahnbrechende Innovationen und schnellere Entscheidungen. Doch mit dem großen Potenzial kommen auch erhebliche Herausforderungen. Die Einführung von KI wirft Fragen der Sicherheit, des Vertrauens und der Compliance auf und setzt Unternehmen unter neuen Druck. Wir bei Dell Technologies haben KI-Sicherheit neu definiert. Unser Ansatz integriert auf einzigartige Weise Datenmanagement, Infrastruktursicherheit und den Schutz von KI-Modellen, um eine umfassende, maßgeschneiderte Lösung bereitzustellen. Ganz gleich, ob Sie neu im Bereich KI sind oder bestehende Lösungen skalieren, unsere End-to-End-Services sorgen für eine schnellere, sicherere und zuverlässigere Einführung von KI.

Sicherheit ist nicht nur eine Aufgabe der IT-Abteilung

Moderne KI-Sicherheit erfordert teamübergreifende Zusammenarbeit. KI-Sicherheit ist ein Teamsport, für den Beiträge und Entscheidungen aus dem gesamten Unternehmen erforderlich sind. Herkömmliche isolierte IT-Betriebsmodelle funktionieren in dieser sich entwickelnden Landschaft nicht mehr. Unser einzigartiger Ansatz bezieht Daten, Infrastruktur, Anwendungen und Modelle in eine einzige, zusammenhängende Strategie ein, die sich an Ihre spezifischen Geschäftsanforderungen anpasst und Ihnen eine ganzheitliche Lösung bietet, mit der Sie stets einen Schritt voraus sind.

Bewältigung der einzigartigen Sicherheitsherausforderungen von KI

Die Einführung von KI bringt komplexe Sicherheits- und Complianceüberlegungen mit sich, die ihre potenziellen Vorteile gefährden können, wie z. B.:

- Datenschutzverletzungen und Verlust von geistigem Eigentum (IP) aufgrund unzureichender Data Protection oder unbefugtem Zugriff
- KI-gestützte Bedrohungen wie gegnerische Angriffe, Modellmanipulation oder Datenvergiftung
- Herausforderungen bei der Verfügbarkeit von KI-Tools, wie z. B. Support-Agents, die ständig einsatzbereit sein müssen
- Sicherheitslücken in der Lieferkette von Drittanbietern, die auf vernetzte Systeme zurückzuführen sind
- Wachsende Angriffsflächen bei der Skalierung von KI-Anwendungen über Hybrid- und Multi-Cloud-Umgebungen hinweg
- Halluzinationen, die zwar kein reines Sicherheitsproblem sind, aber NutzerInnen irreführen können

Wichtigste Vorteile

Mehr Vertrauen und Transparenz: Schützen Sie Daten, geistiges Eigentum und die KI-Integrität, um das Vertrauen der StakeholderInnen aufrechtzuerhalten.

Betriebliche Ausfallsicherheit: Sorgen Sie dafür, dass Ihre erfolgskritischen KI-Systeme betriebsbereit und vor Bedrohungen geschützt bleiben.

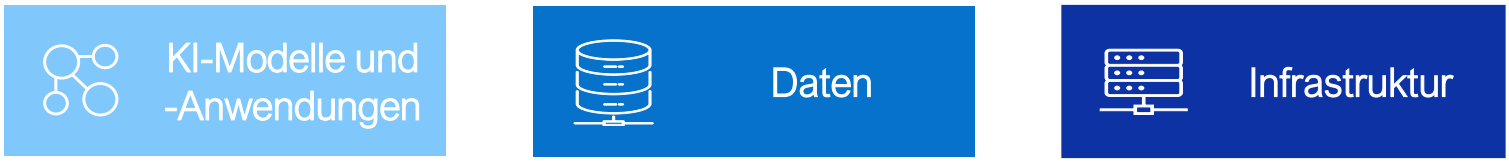
Einhaltung behördlicher Auflagen: Unterstützen Sie die Einhaltung Ihrer branchenspezifischen und behördlichen Anforderungen, um teure Bußgelder und Reputationsschäden zu vermeiden.

Skalierbare Lösungen: Stellen Sie anpassbare KI-Sicherheitsmaßnahmen bereit, die mit Ihrem Unternehmen und seinem Technologiestack wachsen.

Fachkundiger Support und Beratung: Arbeiten Sie mit erfahrenen SicherheitsexpertInnen zusammen, um Ihre Lösung anzupassen und messbare Ergebnisse zu erzielen.

End-to-End-Services für eine maßgeschneiderte Sicherheitsarchitektur

Unsere von Dell entwickelte Sicherheitsarchitektur ist darauf ausgelegt, Ihre individuellen Anforderungen zu erfüllen und eine flexible und zuverlässige Grundlage bereitzustellen. Sie lässt sich nahtlos in die Dell AI Factory einbinden, ermöglicht Zero-Trust-Prinzipien und umfasst fachkundig integrierte Partnertechnologien, um sichere, zukunftsweisende Innovationen voranzutreiben.

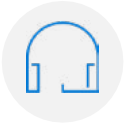


	Merkmale
Beraten Richten Sie Ihre KI-Sicherheit an Unternehmens- und Compliance-Anforderungen aus	• **Security and Resilience for AI Advisory Services** umfassen geschäftliche und technische Workshops zur Entwicklung einer umfassenden Sicherheits- und Verfügbarkeitsstrategie. • **CISO Advisor for AI** stellt einen virtuellen CISO mit KI-Expertenwissen bereit, um Ihre KI-Sicherheitsstrategie in Gang zu bringen. • **Data Security for AI** trägt dazu bei, Datensicherheitsbedrohungen und Risiken für Ihre Daten zu reduzieren.
Implementierung Konzeption und Implementierung von Sicherheitssoftware, um die Sichtbarkeit des KI-Stacks zu erhöhen	• **Security Software Design and Configuration** dient zur Integration von Tools zum Schutz von Zugriffsmanagement, Anwendungen und Netzwerken.
Verwalten Ermöglichen umfassender Transparenz im gesamten Stack, um Bedrohungen schnell zu erkennen und auf sie zu reagieren	• **Managed Detection and Response (MDR)** bietet 24/7 Bedrohungserkennung über Daten, Infrastruktur, Anwendungen und Modelle hinweg. • **Managed AI Firewall** stellt eine isolierte Reihe KI-basierter Schutzmechanismen bereit und überprüft Prompts und Ausgaben auf Policy-Compliance. • **Penetration Testing for AI** simuliert gegnerische Angriffe und deckt Schwachstellen auf. • **Incident Response and Recovery Services** helfen Ihnen, schnell eine Recovery durchzuführen und Ihren Betrieb mit minimaler Unterbrechung wieder aufzunehmen.

Zuversichtlicher Aufbau einer sicheren KI-Zukunft

Die KI-Services für Sicherheit und Resilienz von Dell sind darauf ausgelegt, neue Risiken im Zusammenhang mit der Integration von KI in Ihr Unternehmen zu bewältigen. Unsere Services wurden für die Zusammenarbeit mit Ihren Teams entwickelt, während Sie KI so schnell wie möglich integrieren. Sie bieten Fachwissen für strategische Planung, Lösungsimplementierung und Managed Security Services, um den betrieblichen Aufwand zu verringern, damit Sie mit KI sicher Innovationen schaffen können.

Entdecken Sie Services für Sicherheit und Ausfallsicherheit von Dell Technologies



Kontakt zu einem/r Dell Technologies ExpertIn

Reden Sie mit: #DellTechnologies

DELL Technologies