Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Was ist der Einstein Trust Layer?

Sichere Nutzung von generativer KI

Die meisten Menschen haben Bedenken beim Verwenden von generativer künstlicher Intelligenz wie Chat GPT, Sales AI oder Marketing AI, da sie nicht wissen, was das Large Language Model (LLM) mit ihren Daten macht. Salesforce hat daher das Einstein Trust Layer entwickelt, um die Daten eines Unternehmens trotz Verwendung vieler verschiedener Salesforce KI Tools zu schützen.

Welche Bedenken angemessen sind, wie ein LLM funktioniert und wie Einstein Trust Layer die Bedenken behebt, lesen Sie hier.

Inhalt

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Welche Bedenken in Bezug auf generative KI gibt es?

Menschen haben oft Bedenken und Ängste in Bezug auf die Verwendung generativer Künstlicher Intelligenz (KI) und den Umgang mit ihren Daten. Diese Bedenken können auf verschiedene Faktoren zurückzuführen sein.

Teilweise mag es daran liegen, dass diese Modelle auf großen Mengen an Daten trainiert werden müssen, um effektiv zu funktionieren. Dies bedeutet, dass sensible Informationen, die in den Trainingsdaten enthalten sind, möglicherweise von den Modellen erfasst und verwendet werden können. Menschen befürchten, dass ihre persönlichen Daten, wie beispielsweise private Nachrichten, E-Mails oder Kundendaten von diesen Modellen analysiert und möglicherweise missbraucht werden könnten.

Ein weiterer Grund für die Besorgnis ist die Möglichkeit von Datenlecks oder Sicherheitsverletzungen. Wenn große Mengen an Daten gesammelt und gespeichert werden, besteht immer das Risiko, dass diese Daten in die falschen Hände geraten.

Darüber hinaus besteht die Sorge, dass generative KI-Modelle dazu verwendet werden könnten, gefälschte oder manipulierte Inhalte zu erstellen. Diese Modelle haben die Fähigkeit, menschenähnlichen Text, Bilder oder sogar Videos zu generieren, die schwer von echten Inhalten zu unterscheiden sind. Dies könnte zu einer Verbreitung von Fehlinformationen oder gefälschten Inhalten führen, was das Vertrauen der Menschen in die digitale Welt beeinträchtigen könnte.

Da die GPT-Technologie die Welt im Sturm erobert, ist es nicht verwunderlich, dass diese scheinbar magische Technologie Bedenken hinsichtlich des Datenschutzes und der Legitimität von Informationen aufwirft. Hinzu kommt, dass diese Technologie zunehmend in die Tools eingebettet wird, die wir tagtäglich bei der Arbeit verwenden, und dass die Verantwortlichen für die Plattformen nach Sicherheit suchen. Unternehmensleiter wollen generative KI nutzen, sind aber vorsichtig wegen der Risiken — Datenschutz, Voreingenommenheit und Bedenken hinsichtlich der Datenverwaltung schaffen eine Vertrauenslücke.

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Wie funktioniert ein Large Language Model (LLM)?

In Bezug auf die Funktionsweise eines Large Language Models (LLM) und den Umgang mit Daten ist es wichtig zu verstehen, dass diese Modelle aufgrund ihrer Größe und Komplexität nicht in der Lage sind, gezielt auf bestimmte Daten zuzugreifen oder diese zu identifizieren. LLMs werden in der Regel mit großen Mengen an öffentlich verfügbaren Textdaten trainiert, die aus dem Internet oder anderen Quellen stammen. Die Modelle lernen, indem sie Muster und Zusammenhänge in diesen Daten erkennen, um Texte zu generieren oder Aufgaben wie Übersetzungen oder Textvervollständigungen durchzuführen.

Bei der Verwendung eines LLMs werden die Daten, die von den Benutzern eingegeben werden, normalerweise nicht gespeichert oder dauerhaft verwendet. Die Modelle verarbeiten die Eingabe, generieren eine Ausgabe und geben sie an den Benutzer zurück, ohne die Daten zu speichern. Dies bedeutet, dass die Verwendung eines LLMs in der Regel keine direkte Bedrohung für die Privatsphäre oder Sicherheit der Benutzerdaten darstellt.

Es ist jedoch wichtig zu beachten, dass die Verwendung generativer KI-Modelle nicht ohne Risiken ist. Unternehmen und Entwickler, die solche Modelle einsetzen, sollten angemessene Sicherheitsvorkehrungen treffen, um den Schutz der Daten zu gewährleisten. Dies kann die Anonymisierung oder Verschlüsselung von Daten, die Einhaltung von Datenschutzrichtlinien und die Implementierung von Sicherheitsmaßnahmen umfassen, um Datenlecks oder unbefugten Zugriff zu verhindern.

Insgesamt ist es wichtig, dass die Verwendung generativer KI-Modelle transparent und verantwortungsbewusst erfolgt. Benutzer sollten sich bewusst sein, wie ihre Daten verwendet werden und welche Sicherheitsvorkehrungen getroffen werden, um ihre Privatsphäre zu schützen. Gleichzeitig sollten Unternehmen und Entwickler die Bedenken der Benutzer ernst nehmen und Maßnahmen ergreifen, um den Schutz der Daten zu gewährleisten und das Vertrauen in die Verwendung generativer KI zu stärken.

Dies ist, wo Salesforce ins Spiel kommt: mit dem Einstein Trust Layer.

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Was ist der Einstein Trust Layer?

Als Teil von Salesforce Einstein ist der Einstein Trust Layer ein neuer Industriestandard für vertrauenswürdige Unternehmens-KI. Unternehmen profitieren von generativer KI und können sich gleichzeitig auf den Datenschutz und die Sicherheit verlassen, indem sie verhindern, dass Large-Language-Modelle (LLMs) sensible Kundendaten speichern.

Laut Salesforce waren Vertrauen und Datenschutz der primäre Ausgangspunkt bei der Entwicklung ihrer generativen KI-Funktionen — ein Standpunkt, der Salesforce vom Großteil des Marktes unterscheidet.

Salesforce hat viel getan, um den Datenschutz und die Vertraulichkeit von Daten zu gewährleisten. Ein Beispiel ist die Generierung von Produktbeschreibungen in Commerce AI. Der Prozess findet zum Zeitpunkt der Abfrage (Prompt) statt, wobei die geringste Menge an Daten an die LLMs weitergegeben wird, die die generativen Funktionen betreiben. Dies ist selbstzerstörerisch und hat zur Folge, dass die Kundendaten die Salesforce-Cloud-Produkte, in denen sie gespeichert sind, nie verlassen. Diese Trennung von sensiblen Daten und LLM hilft den Kunden, die Kontrolle über die Data Governance aufrechtzuerhalten und gleichzeitig das immense Potenzial der generativen KI zu nutzen.

Anekdoten von Salesforce-Führungskräften gehen in dieselbe Richtung: Salesforce-Kunden sind eher bereit, generative KI-Technologie zu testen, wenn sie sich des von Salesforce eingebauten “Sicherheitsnetzes” bewusst sind (im Gegensatz zu ihrer Zurückhaltung, wenn es sich um einen offenen API-Aufruf an andere Anbieter handelt).

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Wie funktioniert der Einstein Trust Layer?

- **Keine Datenaufbewahrung:** Die Einstein Trust Layer verhindert, dass Kundendaten außerhalb von Salesforce gespeichert werden. Das bedeutet, dass Prompts und Antworten nicht von LLM-Anbietern gespeichert oder zum Trainieren ihrer Modelle verwendet werden.
- **Feedback-Speicher:** Feedbackschleifen ermöglichen es, die Qualität von Prompts im Laufe der Zeit zu verbessern, wenn Benutzer mit Generativen KI-Funktionen interagieren. Die Einstein Trust Layer sammelt Feedback-Daten, einschließlich der Frage, ob die generierten Antworten hilfreich waren oder nicht, und ob ein Service-Agent diese Antwort schließlich akzeptiert, abgelehnt oder geändert hat.
- **Verschlüsselte Kommunikation:** Die an ein LLM gesendeten Aufforderungen sowie die an Salesforce zurückgesendeten Antworten werden verschlüsselt.
- **Datenzugriffsprüfungen:** Steuert die Eingabeaufforderungen, indem die Ausgaben auf die Daten beschränkt werden, die gemäß den Datenzugriffsrichtlinien des Unternehmens (z. B. Profile, Berechtigungssätze, Rollen und Freigaberegeln) von den Berechtigungen des Benutzers zugelassen sind.
- **Audit-Trail:** Sichere Protokollierung aller Prompts, Ausgaben, Interaktionen und Feedbackdaten, damit Teams von generativer KI profitieren und gleichzeitig ihre Compliance-Anforderungen erfüllen können.

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Wie beeinflusst der Einstein Trust Layer die Zukunft der KI-Sicherheit?

In einer Welt, in der künstliche Intelligenz immer dominanter wird, rückt die Frage, wie wir sicherstellen können, dass unsere Technologien sicher bleiben immer weiter in den Vordergrund. Der Einstein Trust Layer könnte der Schlüssel zur Zukunft der KI-Sicherheit sein. Diese innovative Lösung bietet nicht nur einen Schutzschild gegen Cyber-Bedrohungen, sondern revolutioniert auch die Art und Weise, wie wir Sicherheit in der KI betrachten.

Stellen Sie sich vor, Ihre KI-Systeme hätten einen unsichtbaren Wächter, der ständig auf der Lauer liegt, um potenzielle Gefahren zu erkennen und abzuwehren. Genau das leistet der Einstein Trust Layer. Durch den Einsatz fortschrittlicher Algorithmen und maschinellen Lernens kann er ungewöhnliche Aktivitäten in Echtzeit identifizieren und sofort reagieren. Dies bedeutet, dass Bedrohungen nicht nur erkannt, sondern auch neutralisiert werden, bevor sie Schaden anrichten können.

Zusätzlich setzt der Einstein Trust Layer neue Maßstäbe in puncto Datenschutz. Durch die Verschlüsselung und den kontrollierten Zugriff auf Daten wird sichergestellt, dass nur autorisierte Personen Zugriff haben. Dies stärkt nicht nur die Sicherheit, sondern auch das Vertrauen der Kunden.

Doch das ist noch nicht alles. Der Einstein Trust Layer erhöht die Transparenz und Nachvollziehbarkeit von KI-Entscheidungen. So können Unternehmen nicht nur sicherstellen, dass ihre Daten geschützt sind, sondern auch, dass ihre KI-Systeme ethisch und verantwortungsvoll handeln. So ermöglicht der Einstein Trust Layer die Prüfung von Prompts und Outputs auf Toxizität, damit keine unangemessenen Inhalte verbreitet und Richtlinien zu jeder Zeit eingehalten werden.

Ihre Daten gehören Ihrem Unternehmen. Der Trust Layer verhindert, dass KI-Modelle mit Ihren Daten trainiert werden, da die KI sowohl Ihre Prompts als auch den Output direkt “vergisst”. Sie brauchen sich somit keine Sorgen zu machen, dass andere Unternehmen von Ihren Daten profitieren könnten.

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

In einer Zeit, in der Datensicherheit und ethische KI von größter Bedeutung sind, setzt der Einstein Trust Layer neue Maßstäbe und zeigt, wie die Zukunft der KI-Sicherheit aussehen kann.

Fazit

Der Einstein Trust Layer von Salesforce repräsentiert einen bedeutenden Fortschritt in der Sicherheit und Vertrauenswürdigkeit von KI-Systemen im Unternehmenskontext. Als Antwort auf wachsende Bedenken bezüglich Datenschutz und Sicherheit bei der Nutzung generativer KI, bietet diese Lösung einen robusten Schutzschild für sensible Kundendaten. Durch Funktionen wie Zero-Retention, verschlüsselte Kommunikation und strenge Zugriffskontrollen adressiert der Trust Layer kritische Sicherheitsaspekte, ohne die Leistungsfähigkeit der KI einzuschränken.

Die Integration in die Salesforce-Plattform ermöglicht Unternehmen, das Potenzial generativer KI voll auszuschöpfen, während gleichzeitig höchste Sicherheitsstandards gewahrt bleiben. Mit Blick auf die Zukunft setzt der Einstein Trust Layer neue Maßstäbe für ethische und verantwortungsvolle KI-Nutzung in der Geschäftswelt.

Erfahren Sie hier mehr über den Einstein Trust Layer:
https://www.salesforce.com/de/artificial-intelligence/trusted-ai/

Autor: Lea Schäfer, Online Marketing
Herausgeber: comselect GmbH
Veröffentlichung: Juli 2024
Lesedauer: 4 Minuten

Kontakt

Haben wir Ihr Interesse geweckt?

Seit 2002 unterstützen wir unsere Kunden bei der Einführung und Anpassung von Salesforce auf individuelle Unternehmensbedürfnisse. Mit dieser Erfahrung können wir sicher auch Ihnen ein zuverlässiger Partner sein. Ob Konzern, Mittelstand oder KMU – wir kennen die Herausforderungen in vielen Branchen und entwickeln auch für Sie die optimale Lösung.

Nehmen Sie mit uns Kontakt auf:

Comselect Gesellschaft für Relationship Management mbH

Bernd Bittner, Sales Director CRM Services

Telefon: 0621 / 76133 500

Email: info@comselect.de

Web: https://comselect.de

Wir über uns.

comselect ist ein inhabergeführtes Unternehmen mit Hauptsitz in Mannheim und Niederlassung in Augsburg. Unsere Experten aus den Bereichen CRM Consulting, künstliche Intelligenz, digitales Marketing und Prozesse haben sich auf die Umsetzung komplexer Projekte, von der strategischen CRM Beratung, über die Konzeption bis zur Umsetzung, spezialisiert. Seit 2002 sind wir der führende Partner für den deutschen Mittelstand. Unser Branchenschwerpunkt ist die herstellende Industrie. Unsere Berater treffen Sie in Hamburg, Berlin, Düsseldorf, Frankfurt, München, Stuttgart.