

CIO-Guide zur Minimierung von KI-Risiken



Übersicht

- 3 **Einführung**
- 4 **Kapitel 1:** Neue Herausforderungen durch agentenbasierte Workflows
- 5 **Kapitel 2:** Vier wichtige KI-Risikovektoren
- 6 **Kapitel 3:** Warum traditionelle Governance zu kurz greift
- 7 **Kapitel 4:** Ein analytischer Ansatz zur KI-Risikominderung
- 8 **Kapitel 5:** ROI mit Pendo nachweisen
- 9 **Fazit**

Einführung

KI ist unvermeidlich. Aber ihr Potenzial birgt ernsthafte Risiken.

KI, große Sprachmodelle (LLMs) und autonome Agenten verändern bereits die Geschäftswelt. Wir treten in eine Ära ein, in der Wissensarbeiter weniger Zeit mit administrativen und sich wiederholenden Aufgaben verbringen und mehr Zeit damit, Werte für das Unternehmen zu schaffen.

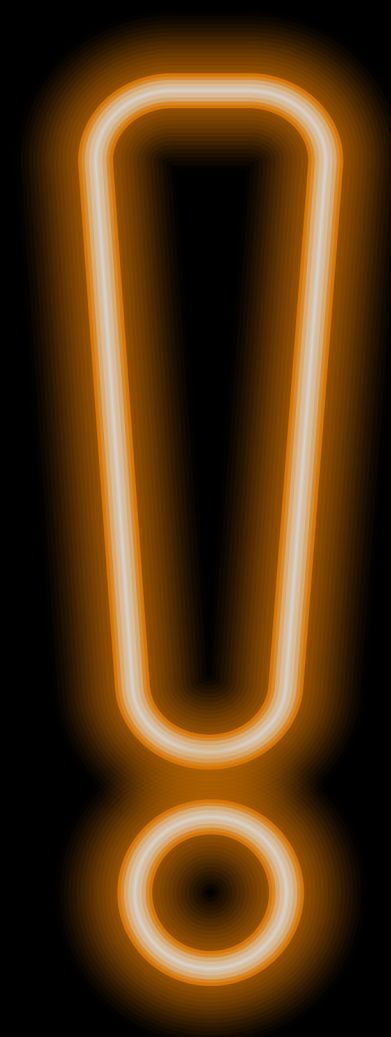
Führungskräfte erkennen das Potenzial und sind voll dabei. Eine [PwC-Umfrage](#) ergab, dass fast die Hälfte der Fortune-1000-Unternehmen KI vollständig in ihre Produkte integriert haben.

Die potenziellen Steigerungen bei Produktivität und Effizienz sind enorm – aber ebenso die potenziellen Compliance-, Sicherheits- und Betriebsrisiken. CIOs müssen ein Gleichgewicht finden zwischen zu schnellem Handeln, das eine Katastrophe heraufbeschwört, und zu langsamem Handeln, das sie hinter ihre Konkurrenten zurückfallen lässt.

Traditionelle Governance-Modelle sind zu starr, risikoscheu und ausschussgesteuert, um mit dem Tempo der KI-Innovation Schritt zu halten. Sie benötigen Transparenz, Flexibilität und Kontrolle durch Tools, die sich so schnell entwickeln wie Ihr Tech-Stack.

Dieser Leitfaden untersucht die wichtigsten Risiken, die KI mit sich bringt, und wie man sie mindern und minimieren kann. Wir zeigen, wie Unternehmen diese Ideen bereits jetzt in die Praxis umsetzen.

So stellen Sie sicher, dass Ihre KI-Implementierung transformativ und nicht destruktiv ist.



Kapitel 1

Neue Herausforderungen durch agentenbasierte Workflows

Die neueste KI-Disruption sind agentenbasierte Workflows – autonome KI-Agenten, die Aufgaben ohne menschliches Eingreifen übernehmen.

Der Hype um agentenbasierte Workflows erreicht seinen Höhepunkt. In einer [Umfrage unter 1.500 IT-Führungskräften](#) gaben 96 % an, ihren Einsatz von KI-Agenten im kommenden Jahr erhöhen zu wollen. Diese Investitionen machen einen beträchtlichen Teil der prognostizierten IT-Budgets aus: Eine weitere [globale Umfrage](#) ergab, dass ein Drittel der Unternehmen im Jahr 2025 erwartet, 25 Millionen US-Dollar oder mehr für KI auszugeben.

Es lässt sich nicht leugnen, dass KI-Agenten unglaublich nützlich sein können. Sie können Kundenanfragen beantworten, Berichte erstellen und interne Prozesse selbstständig ausführen. Das bedeutet, dass Ihre Teams repetitive Aufgaben an die KI auslagern können, sogar komplexe Workflows, die über mehrere Anwendungen hinweg ausgeführt werden.

Doch die Autonomie, die agentenbasierte Workflows so attraktiv macht, birgt auch neue Risiken. KI-Agenten könnten sensible Daten auf nicht konforme Weise zugreifen und verwenden, z. B. Informationen Personen oder Parteien offenlegen, die keine Zugriffsberechtigung haben. Agenten könnten auch falsche Informationen geben, die Ihr Unternehmen in ethische oder sogar rechtliche Schwierigkeiten bringen könnten.

Zum Beispiel hat der Chatbot von Air Canada im Laufe eines Chats einen [Gutschein erfunden](#). Als die Fluggesellschaft sich weigerte, den Rabatt einzulösen, verklagte der Reisende sie – und gewann. Das Gericht entschied, dass Air Canada rechtlich für das verantwortlich war, was ihr Chatbot den Kunden sagte.

Kapitel 2

Vier wichtige KI-Risikovektoren

Da KI immer stärker in den täglichen Betrieb integriert wird, müssen CIOs vorgewarnt und vollständig darauf vorbereitet sein, neue Risiken anzugehen. Diese fallen in vier große Kategorien:

- 1 Sicherheitslücken.
- 2 Compliance-Fehler.
- 3 „Schatten-KI“
- 4 Software-Wildwuchs und Erfahrungserosion.

CIOs sind es gewohnt, Risiken wie diese zu managen, aber autonome Agenten erfordern mehr Aufsicht als die durchschnittliche SaaS-Lösung. Ihre Steuerung erfordert eine kontinuierliche, kontextbezogene Einsicht in ihr Verhalten.

1. Sicherheitslücken.

KI-Agenten können sowohl innerhalb als auch über Anwendungen hinweg arbeiten, was sie zu Hauptzielen für Ausnutzung macht. Sie sind normalerweise nicht-deterministisch, was es schwierig macht, traditionelle Sicherheitsbedrohungsmodelle oder Entwurfsprüfungsgrundsätze anzuwenden. Ohne ausreichende Aufsicht könnten sie zum Export von Daten, zu nicht nachvollziehbaren Änderungen und sogar zur Gewährung von Administratorrechten an böswillige Akteure verwendet werden.

2. Compliance-Fehler.

Agenten können compliance-erforderliche Schritte in Workflows übersehen. Sie könnten PII falsch handhaben, das Vertrauen Ihrer Kunden verletzen und potenziell Datenschutzgesetze brechen. Sie könnten es versäumen, Prozesse zu dokumentieren, die eine elektronische Spur erfordern, oder Daten verwerfen, die Ihr Unternehmen gesetzlich aufbewahren muss.

3. „Schatten-KI.“

So wie Mitarbeiter nicht autorisierte Software verwenden, können Teams jetzt KI-Tools ohne IT-Aufsicht in Betrieb nehmen, wodurch fragmentierte und unregierbare Systeme entstehen.

4. Software-Wildwuchs und Erfahrungserosion.

Die Benutzererfahrung kann sich verschlechtern, wenn sich KI-Tools ausbreiten. Überlappende Tools und unklare Workflows frustrieren Mitarbeiter und untergraben die Produktivität, während sie gleichzeitig wertvolles IT-Budget verschwenden können.

Kapitel 3

Warum traditionelle Governance zu kurz greift

Die meisten Organisationen werden versuchen, diese Risiken mit bewährten Methoden zu managen, die für andere Arten von Software funktionieren. Sie könnten mehr Mitarbeiterschulungen anordnen, den Zugriff auf Tools einschränken und Seiten mit Nutzungsrichtlinien entwerfen. Aber obwohl diese Bemühungen ein notwendiger Teil der rechtlichen und regulatorischen Compliance für Mitarbeiter sind, sind sie für agentenbasierte Workflows unzureichend.

Während Sie einen KI-Agenten sicherlich mit Ihrer Dokumentation zur Sicherheitsbewusstseins schulen können, gibt es keine Garantie, dass die Schulung effektiv ist. Richtlinien können nicht jede Eventualität abdecken. Manuelle Audits können mit einem Verhalten, das sich autonom von Moment zu Moment ändern kann, nicht mithalten.

Agentenbasierte Workflows erfordern eine Aufsicht, die:

Echtzeit ist. Wissen Sie, wie Ihre Agenten funktionieren und mit Benutzern interagieren.

- **Verhaltensorientiert ist.** Überwachen Sie Aktionen, nicht nur Ergebnisse.
- **Handlungsfähig ist.** Haben Sie die Möglichkeit, einzugreifen und zu verbessern.

Pendo hat eine nachweisliche Erfolgsbilanz bei der Unterstützung von CIOs bei der Reduzierung softwarebezogener Risiken. So helfen wir Unternehmen, die Herausforderungen der agentenbasierten Ära zu meistern.

Kapitel 4

Ein analytischer Ansatz zur KI-Risikominderung

Was wäre, wenn Sie Ihre KI-Agenten auf dieselbe quantitative, dateninformierte Weise analysieren könnten wie die Benutzeraktivität? Was wäre, wenn Sie untersuchen könnten, wie Ihre Mitarbeiter KI-Agenten verwenden, riskantes Verhalten identifizieren und Anleitungen zur Minderung anwenden könnten?

Pendo Agent Analytics wurde entwickelt, um das Verhalten von Agenten, die Sie entwickeln und Agenten, die Sie kaufen, zu analysieren, um sicherzustellen, dass sie die Produktivität und den Umsatz steigern, ohne Risiken einzuführen. Es ist einfach zu sehen, wie Benutzer mit KI-Agenten interagieren – ob Benutzer Wert aus diesen KI-Helfern ziehen, wofür sie verwendet werden und ob sie Wert schaffen.

Für Agenten, die Sie entwickeln, hilft Pendo Agent Analytics, die Akzeptanz zu erhöhen, Ihre KI-Roadmap-Entscheidungen zu verbessern und Ihre technische Arbeit an KI-Agenten direkt mit Geschäftsergebnissen zu verbinden. Für Agenten, die Sie kaufen, kann Pendo auch dazu beitragen, die Akzeptanz zu fördern, die Produktivität zu verbessern, die KI-Nutzung Ihres Unternehmens zu verstehen und Risiken zu reduzieren.

Pendo wurde entwickelt, um Ihnen zu helfen, den vollen Wert Ihrer Software zu erschließen. Jetzt erstreckt sich diese Funktionalität auch auf agentenbasierte Workflows.

KUNDENSTORY

Thomson Reuters' Steuer- und Buchhaltungsabteilung führte eine KI-gestützte Suchmaschine für ihre Checkpoint Edge-Plattform ein. Sie mussten verstehen, wie Menschen mit der neuen Funktionalität interagierten, um die Relevanz der Suchmaschine zu verbessern.

Sie verwendeten Pendo, um quantitative Einblicke in das Sucherlebnis zu gewinnen, und korrelierten die Ergebnisse anschließend mit den NPS-Werten, um ein vollständiges Bild zu erhalten. Diese Daten befähigten ihr Entwicklungsteam, die KI-Fähigkeiten zu verbessern und sicherzustellen, dass die Nutzer bei jeder Suche die relevantesten Inhalte erhielten.

Kapitel 5

ROI mit Pendo nachweisen

Verschwendete Ausgaben sind bei jeder Softwareanschaffung ein großes Risiko – und KI-Lösungen bilden hier keine Ausnahme. Wenn Ihr Unternehmen über einen fragmentierten Tech-Stack mit Dutzenden von KI-Anwendungen verfügt, kann es bereits eine Herausforderung sein, einfach herauszufinden, was genutzt wird – und was nicht.

Pendo macht es einfacher, die entscheidenden Fragen zu beantworten, die CIOs in Bezug auf die agentische Einführung haben:

- Sparen Agenten den Nutzern Zeit bei wichtigen Workflows und Prozessen?
- Senken sie Kosten und helfen, den Umsatz zu steigern?
- Entlasten sie Teams, sodass diese an höherwertigen Aufgaben arbeiten können?
- Steigern sie Ergebnisse wie abgeschlossene Aufgaben und Conversions?

Mit Pendo's KI-gestützten Analysen erhalten Sie volle Transparenz bei all diesen Fragen – und die Werkzeuge, um die Erkenntnisse direkt in Maßnahmen umzusetzen, alles in einer nahtlosen Lösung.

KUNDENSTORY

Demandbase, eine führende Go-to-Market-Plattform, integrierte KI-Agenten in ihre Plattform, um Kunden dabei zu unterstützen, schneller zu arbeiten und mehr Pipeline abzuschließen. Dafür mussten sie beobachten, wie Nutzer mit den Agenten interagierten, und kontextbezogenes Feedback einholen.

Pendo machte es einfach, die benötigten Einblicke zu gewinnen. „Wir erhalten Feedback direkt im Produkt, genau in dem Moment, in dem die Nutzer mit den Agenten interagieren“, sagte Chad Holdorf, VP of Product bei Demandbase.

„Job zu machen, ob es tatsächlich die Pipeline vorantreibt. Diese Art von Feedback ist entscheidend, um die richtigen Agenten zu entwickeln und sie schnell zu verbessern.“



Fazit

KI intelligent einführen

Es ist klar: KI ist mehr als nur ein Trend oder „das nächste große Ding“. Sie stellt möglicherweise einen grundlegenden Wandel in der Arbeitsweise Ihres Unternehmens dar. CIOs haben die Aufgabe, ihre Organisationen klug und sicher durch diese Transformation zu führen.

Pendo ist bereit, Sie durch das agentische Zeitalter zu begleiten. Mit Pendo Agent Analytics und der gesamten Pendo-Plattform erhalten Sie Einblicke sowohl in das Verhalten der Agenten als auch in die Interaktionen Ihrer Nutzer mit der Technologie – und können die richtigen Maßnahmen ergreifen, um beides zu optimieren.

Letztlich hilft Pendo dabei, KI-bezogene Risiken zu reduzieren und das volle Potenzial agentischer Workflows für Ihr Unternehmen auszuschöpfen.

Melden Sie sich noch
heute an und nutzen
Sie Pendo kostenlos.