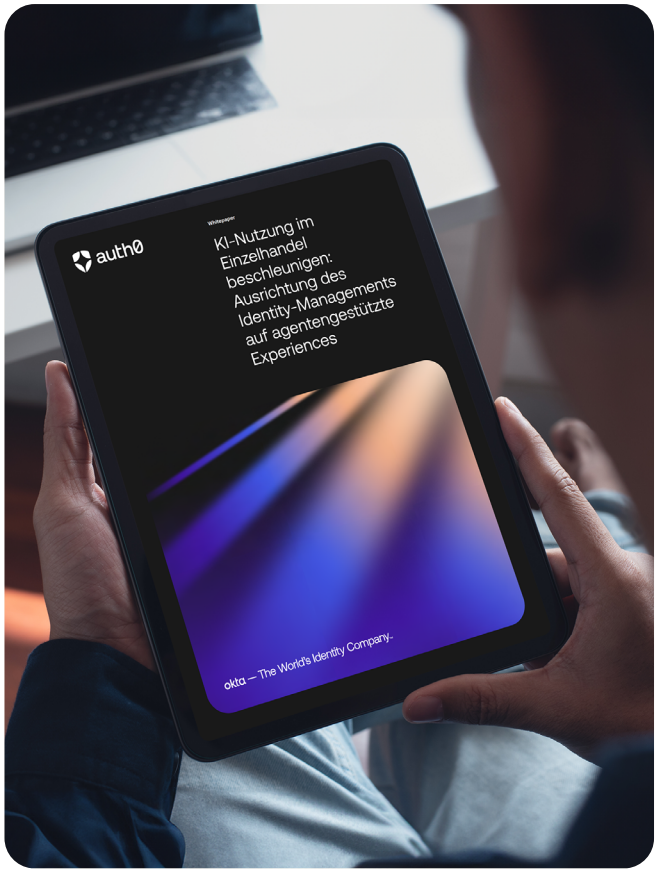
Checkliste zur Vorbereitung auf KI und Identity-Management

Wie bereit ist der Identity-Stack Ihres Einzelhandels-unternehmens für KI-Agenten, Automatisierung und Maschine-zu-Maschine-Interaktionen?

KI-Agenten sind bereits in Ihrer gesamten Einzelhandels-umgebung aktiv. Die meisten Teams können jedoch nicht zuverlässig kontrollieren, worauf sie Zugriff haben.

Anhand dieser Checkliste können Sie analysieren, ob Ihre Identity-Ebene die im Auftrag Ihrer Kundschaft, Angestellten und internen Services agierenden KI-Systeme zuverlässig unterstützen kann.

Überprüfen Sie jeden Punkt, der für Ihre aktuelle Umgebung in Frage kommt. Wenn Sie sich nicht sicher sind, gehen Sie davon aus, dass eine Sicherheitslücke vorhanden ist.



1. Agentenidentität und Zuständigkeit

- ☐ Haben Sie einen Überblick über alle KI-Agenten, Copiloten und automatisierten Services in Ihrer Umgebung?
- ☐ Ist jeder Agent an bestimmte Benutzende, Systeme oder Geschäftsfunktionen gebunden?
- ☐ Können Sie alle Agentenaktionen klar einer bestimmten Absicht (Benutzende, Workflow oder System) zuordnen?
- ☐ Verfügen Sie über ein aktuelles Inventar oder eine Registrierung für aktive nicht-menschliche Identitäten?

2. Authentifizierung und Delegierung

- ☐ Authentifizieren sich KI-Agenten mit modernen Standards wie OAuth 2.0 oder OIDC anstelle von gemeinsam genutzten Anmeldedaten?
- ☐ Verwenden Agenten, die im Namen von Benutzenden handeln, einen sicheren Token-Austausch oder delegierte Identity-Abläufe?
- ☐ Bleibt der Benutzerkontext erhalten, wenn ein Agent systemübergreifend Aktionen ausführt?
- ☐ Können Sie Agenten widerrufen oder erneut authentifizieren, ohne den gesamten Workflow zu unterbrechen?

3. Token- und Anmeldedaten-Management

- ☐ Sind API-Token kurzlebig, umfassen sie Definitionen zum Berechtigungsbereich und werden sie automatisch rotiert?
- ☐ Sind in Code, Protokollen und Pipelines keine Secrets gespeichert?
- ☐ Vermeiden Agenten die Verwendung von festcodierten API-Keys oder statischen Anmeldedaten?
- ☐ Können Sie alle von KI-Systemen verwendeten Token zentral verwalten und prüfen?

4. Autorisierung und Richtliniendurchsetzung

- ☐ Erzwingen Sie Least-Privilege-Zugriff für alle KI-Agenten?
- ☐ Werden Berechtigungen zum Zeitpunkt der Anfrage überprüft und nicht fest in der Anwendungslogik codiert?
- ☐ Können Sie festlegen, welche Aktionen ein Agent basierend auf dem Kontext (Benutzender, Transaktion, Risiko) ausführen kann?
- ☐ Werden Aktionen mit hohem Risiko (z. B. Rückerstattungen, Account-Änderungen) durch zusätzliche Genehmigungen oder Richtlinienprüfungen abgesichert?

5. Datenzugriff und RAG-Kontrollen

- ☐ Erzwingen Sie feingranulare Zugriffskontrollen für Daten, die von KI-Systemen abgerufen werden?
- ☐ Können Sie einschränken, auf welche Dokumente, Datensätze oder Felder ein Agent zugreifen kann?
- ☐ Sind KI-Antworten auf Daten beschränkt, die der Benutzende, in dessen Namen der Agent handelt, sehen darf?
- ☐ Verhindern Sie die Kompromittierung vertraulicher Daten in Prompts, Protokollen oder Modellausgaben?

6. Transparenz und Überwachung

- ☐ Können Sie nachverfolgen, welche Aktionen jeder KI-Agent über Systeme und APIs hinweg durchführt?
- ☐ Protokollieren Sie, welche Identität, welches Token und welche Richtlinie jede Aktion ermöglicht hat?
- ☐ Können Sie ungewöhnliches oder auffälliges Agentenverhalten in Echtzeit erkennen?
- ☐ Haben Sie eine Möglichkeit, einen sich falsch verhaltenden Agenten schnell zu deaktivieren oder zu isolieren?

7. Integrations- und Kontrollebene

- ☐ Verwaltet Ihre Identity-Ebene zentral alle Anwendungen, APIs und KI-Systeme?
- ☐ Können Sie einheitliche Authentifizierungs- und Autorisierungsrichtlinien für alle Agenten anwenden?
- ☐ Lässt sich Ihr Identity-System ohne benutzerdefinierte Workarounds in KI-Plattformen, APIs und Datenquellen integrieren?
- ☐ Können Entwicklungsteams die Identity-Logik (Richtlinien, Hooks, Workflows) erweitern, ohne Kernsysteme neu zu schreiben?

Punktzahl:

- **24–28 Kästchen angekreuzt:** Ihre Identity-Ebene ist gut geeignet, um KI-Agenten sicher und im großen Umfang zu unterstützen.
- **16–23 Kästchen angekreuzt:** Sie haben eine solide Grundlage, aber mit zunehmendem KI-Einsatz können Lücken auftreten.
- **Weniger als 16 Kästchen:** Ihre Identity-Ebene ist möglicherweise nicht bereit, KI-Systeme im Produktivbetrieb sicher zu unterstützen.

Möchten Sie mehr Details erfahren?

Erfahren Sie, wie Auth0 Teams dabei unterstützt, KI-Agenten mit Authentifizierung, Token-Verwaltung und feingranularer Autorisierung abzusichern.