KI-Assistent – Technisches Dokument zum Thema Sicherheit

Veröffentlicht: April 2026 | Verbreitung: Öffentlich

Kurze Zusammenfassung

Der KI-Assistent ist eine in Jamf Pro, Jamf Account und Jamf Protect integrierte dialogbasierte Schnittstelle, die auf der Grundlage von Claude (Anthropic) über AWS Bedrock bereitgestellt wird. Es bietet Produktionswerkzeuge für Bestandsabfragen, Konfigurationsanalysen, Konformitätsprüfungen und den Wissensabruf.

Dieses Dokument beschreibt die Sicherheitsarchitektur, die Verfahren zum Umgang mit den Daten und die Datenschutzmechanismen, die die Nutzung des KI-Assistenten in allen Jamf Cloud-Regionen (USA, EU, APAC) regeln.

Der KI-Assistent basiert auf vier Sicherheitsprinzipien, die jeweils auf architektonischer Ebene und nicht nur auf der Ebene der Richtlinien oder Eingabeaufforderungen durchgesetzt werden: standardmäßige Deaktivierung, Zugriffskontrolle nach dem Prinzip der geringsten Berechtigungen, Durchsetzung des Lesezugriffs auf API-Ebene sowie transparente und nachvollziehbare Antworten. AWS Bedrock Guardrails bieten umgebungsübergreifende Inhaltsüberwachung und Prompt-Injection-Erkennung.

Übersicht der Architektur

Infrastruktur

Der KI-Assistent kann in allen Jamf Cloud-Regionen genutzt werden. Die Kundendaten werden in der Region verarbeitet, in der die jeweilige Jamf-Umgebung gehostet wird, und werden nicht über regionale Grenzen hinweg übertragen.

Region	AWS Bedrock-Region	Status
Vereinigte Staaten	US-EAST-1	Produktivsystem
Europäische Union	EU-CENTRAL-1	Produktivsystem
Asien-Pazifik	AP-NORTHEAST-1	Produktivsystem

Modell

Der KI-Assistent nutzt Claude (Anthropic) via AWS Bedrock. Bedrock stellt die Inferenzschicht zwischen der Infrastruktur von Jamf und dem Modell von Anthropic bereit. Informationen zur aktuellen Modellversion finden Sie im Jamf Learning Hub.

Beziehung zu Unterauftragsverarbeitern von Anthropic: Anthropic empfängt keine Kundendaten und hat auch keinen Zugriff darauf. Die Modellinferenz erfolgt innerhalb der AWS Bedrock-Infrastruktur, die in der AWS-Umgebung von Jamf betrieben wird. Anfragen der

Kunden, Tool-Ergebnisse und der Konversationskontext werden in Bedrock verarbeitet und nicht an Anthropic übermittelt. Weitere Informationen dazu, wie AWS Bedrock den Datenschutz und die Datensicherheit handhabt, finden Sie in der Dokumentation zum Datenschutz bei AWS Bedrock.

Sicherheitseigenschaften von AWS Bedrock:

- Kundendaten werden nicht zum Trainieren oder Feinabstimmen der Modelle von Anthropic verwendet
- Die Daten werden innerhalb der Region verarbeitet und verlassen die AWS-Region, in der die Umgebung des Kunden gehostet wird, nicht.
- SOC 2 Typ II-konform
- Die AWS-Sicherheitsmaßnahmen für Unternehmen gelten für alle Inferenzanfragen.

Modellaktualisierungen: Jamf verwaltet die Modellversionierung über AWS Bedrock. Die aktuelle Modellversion wird im Jamf Learning Hub gepflegt – Unternehmen mit Anforderungen an das Änderungsmanagement sollten den Learning Hub auf Änderungen der Modellversion überwachen.

Tool-Architektur

Der KI-Assistent nutzt eine Architektur zum Aufruf von Tools: Wenn ein Benutzer eine Anfrage sendet, ermittelt das Modell, welche Tools aufgerufen werden sollen, führt diese unter Verwendung der bestehenden Berechtigungen des Benutzers über bestimmte Jamf-APIs aus und fasst die Ergebnisse zu einer Antwort zusammen.

Alle Tools sind schreibgeschützt. KI-Assistenten-Tools lassen sich in fünf Kategorien einteilen: Wissensabruf (Jamf-Dokumentation und Wissensdatenbank), Zugriff auf Konfigurationen (Richtlinien, Profile, Skripte, Entwürfe usw.), Bestandsabfragen (Gerätedaten – Mac und Mobilgeräte), Prüfung der Konformität (Abgleich mit CIS, NIST und DoD STIG, usw.) sowie Sicherheitsinformationen (Risikobewertungen für mobile Apps). Die Jamf Protect-Tools (Alarmanalyse, Malware-Abfrage) sind als eingeschränkte Betaversion verfügbar. Den aktuellen Werkzeugkatalog mit Angaben zur Verfügbarkeit und zu den Produktanforderungen finden Sie im Jamf Learning Hub.

Datenströme von Drittanbietern: Drei Tools greifen auf externe Dienste außerhalb der Jamf-Infrastruktur zu. Diese Integrationen werden aus Gründen der Transparenz dokumentiert.

- **Apple OS Lookup** fragt die API des „Global Device Management Framework“ (GDMF) von Apple (gdmf.apple.com) ab, einen öffentlichen Endpunkt von Apple. Dabei werden keine Kundendaten übermittelt – das Tool ruft ausschließlich öffentlich zugängliche Informationen zu Apple-Betriebssystemversionen ab.
- **App Lookup** fragt die iTunes Search API (itunes.apple.com) als Fallback für App-Versionen und Patch-Informationen ab. Dabei werden keine Kundendaten übermittelt – das Tool ruft ausschließlich öffentlich zugängliche App-Metadaten ab.

- **Mobile App Risk** fragt die MARI-Datenbank (Mobile Application Risk Intelligence) von NowSecure ab, um Sicherheitsbewertungen abzurufen. Es werden lediglich die Daten zur Store-ID der App (z. B. die iOS-Bundle-ID) und zur Plattform (iOS oder Android) übermittelt. Es werden keine Gerätedaten, Benutzeridentitäten oder Unternehmensinformationen übertragen.

Grundsätze der Sicherheitsgestaltung

Standardmäßig deaktiviert: Der KI-Assistent ist für alle Organisationen deaktiviert, bis er von einem Administrator im Jamf-Account ausdrücklich aktiviert wird. Einzelne Tool-Gruppen müssen separat aktiviert werden – die Aktivierung des KI-Assistenten-Kerns führt nicht automatisch zur Aktivierung der Jamf Pro-Tools oder zukünftiger Produktintegrationen. Den Benutzern stehen die KI-Funktionen erst zur Verfügung, wenn ihre Organisation sich ausdrücklich dafür entschieden hat, diese zu aktivieren, und Administratoren können jede Tool-Gruppe jederzeit deaktivieren.

Zugriffskontrolle nach dem Prinzip der geringsten Berechtigungen: Alle Tool-Abfragen werden unter den Berechtigungen des authentifizierten Benutzers ausgeführt und übernehmen dabei die bestehenden RBAC-Kontrollen von Jamf Pro unverändert. Der KI-Assistent erweitert weder die Berechtigungen noch greift er auf Daten zu, auf die der Benutzer nicht bereits direkt zugreifen kann. Ein Benutzer, der keine Berechtigung zum Anzeigen einer Richtlinie hat, kann diese auch nicht über den KI-Assistenten abrufen.

Durchsetzung der Schreibschutzfunktion auf API-Ebene: Der KI-Assistent ruft die Jamf Pro-APIs mithilfe des Sitzungstokens des authentifizierten Benutzers auf – es gibt kein separates Dienstkonto mit erweiterten Anmeldedaten. Alle von KI-Assistenten-Tools ausgegebenen API-Aufrufe sind GET-Anfragen. Kein Tool im System sendet eine POST-, PUT-, PATCH- oder DELETE-Anfrage an Jamf Pro. Es handelt sich hierbei um eine architektonische Einschränkung, die auf der Implementierungsebene durchgesetzt wird – nicht um eine Anweisung auf der Eingabeebene oder eine Richtlinie, die durch geschickte Eingabeaufforderungen außer Kraft gesetzt werden könnte. Unabhängig davon, wie eine Abfrage aufgebaut ist, kann der KI-Assistent keine Gerätekonfigurationen ändern, keine Richtlinien bereitstellen, keine Apps entfernen und keine Registrierungsstatus ändern.

Transparente, nachvollziehbare Antworten: Jede Antwort legt ihre Quellen offen, sodass Administratoren die Antworten anhand von verbindlichen Unterlagen überprüfen können. Die an das Modell zurückgegebenen Tool-Ergebnisse liegen als strukturierte Daten und nicht als Freitext vor, sodass jede Antwort bis zu ihrer Quelle zurückverfolgt werden kann.

„Guardrails“ von Bedrock: AWS Bedrock Guardrails werden in allen KI-Assistenten-Umgebungen bereitgestellt. Die „Guardrail“-Konfiguration umfasst eine Inhaltsüberwachung für verschiedene Risikokategorien (Gewalt, sexuelle Inhalte, Hassreden, Beleidigungen, Fehlverhalten) sowie hochsensible Prompt-Injection-Erkennung. Alle Guardrail-Ereignisse werden nachverfolgt und protokolliert, wodurch ein vollständiges Prüfprotokoll der relevanten Ein- und Ausgaben entsteht.

Datenverarbeitung

Datenfluss

Wenn ein Benutzer eine Abfrage sendet, passiert Folgendes:

1. **Abfrageverarbeitung:** Die in natürlicher Sprache formulierte Abfrage des Benutzers wird vom Backend des KI-Assistenten empfangen.
2. **Tool-Ausführung:** Die entsprechenden Tools fragen die Jamf-APIs unter Verwendung der Berechtigungen des authentifizierten Benutzers ab.
3. **Zusammenstellung der Informationen:** Die Anfrage des Benutzers, relevante Tool-Ergebnisse und der aktuelle Konversationsfaden werden für die Inferenz vorbereitet.
4. **Modellinferenz:** Die Inferenzanfrage wird von AWS Bedrock verarbeitet und eine Antwort generiert.
5. **Übermittlung der Antwort:** Die generierte Antwort wird dem Benutzer in der Oberfläche von Jamf angezeigt.

Welche Daten werden während der Inferenz verarbeitet?

Datentyp	Verarbeitet durch die Inferenzebene	Anmerkungen
Benutzeranfrage	Ja	Die gestellte Frage in natürlicher Sprache
Ergebnisse des Tools	Ja	Inventardaten, für die Abfrage relevante Konfigurationsdetails
Chatverlauf	Ja	Vollständiger Thread-Verlauf der aktuellen Unterhaltung, aus dem persistenten Speicher geladen; wird 30 Tage lang aufbewahrt
Anmeldedaten für Benutzer oder Tokens	Nein	Niemals im Modellkontext enthalten
Gesamter Datenbankinhalt	Nein	Es werden nur abfragerelevante Ergebnisse angezeigt

Datenresidenz

Der KI-Assistent hält sich an die regionalen Datengrenzen von Jamf. Inferenzanfragen werden an die AWS Bedrock-Bereitstellung in derselben Region wie die Jamf-Umgebung des Kunden weitergeleitet:

- **Kunden in den USA:** Die Daten werden in AWS US-EAST-1 verarbeitet
- **Kunden in Europa:** Daten werden in AWS EU-CENTRAL-1 verarbeitet
- **Kunden aus der APAC-Region:** Die Daten werden in AWS AP-NORTHEAST-1 verarbeitet

Gerätebestände, Konfigurationsdaten und andere kundenspezifische Daten werden nicht zwischen den Regionen übertragen.

Hinweis zum Wissensabruf: Der Wissensabruf fragt nur die Jamf-Dokumentation ab – er greift nicht auf den Gerätebestand, Konfigurationsdetails oder andere kundenspezifische Daten. Alle Anfragen an den KI-Assistenten, einschließlich des Wissensabrufs, werden in der dem Kunden zugewiesenen Region verarbeitet.

Sitzungsisolierung

Jedes Gespräch mit dem KI-Assistenten ist auf den authentifizierten Benutzer und dessen Organisation beschränkt. Der Inhalt des Gesprächs wird weder zwischen einzelnen Benutzern noch zwischen Kundenorganisationen weitergegeben. Eine Abfrage einer Organisation kann keine Daten zum Bestand oder Konfigurationsdetails einer anderen Organisation offenlegen.

Chatverläufe werden 30 Tage lang gespeichert und anschließend automatisch und dauerhaft gelöscht. Die Aufbewahrung wird auf der Speicherebene über die DynamoDB-TTL durchgesetzt – nicht durch einen geplanten Bereinigungsvorgang, der verschoben oder übersprungen werden kann. Jede Unterhaltung ist nur für den Benutzer und die Organisation zugänglich, die sie erstellt hat. Die Gesprächsdaten werden ausschließlich in der Infrastruktur von Jamf gespeichert – Anfragen und Antworten werden von AWS Bedrock oder Anthropic über die Inferenzanfrage hinaus weder protokolliert noch aufbewahrt.

Aufbewahrung und Prüfprotokolle

Der **Inhalt der Konversation** wird 30 Tage lang gespeichert. Nach 30 Tagen werden die Chat-Daten gelöscht und können nicht wiederhergestellt werden.

Die **Prüfprotokolle** werden im Jamf Account unter „Aktivitätsverlauf“ → „KI-Assistent“ geführt. Das Prüfprotokoll erfasst alle administrativen Änderungen an der Konfiguration des KI-Assistenten, darunter:

- KI-Assistent aktiviert oder deaktiviert
- Werkzeuggruppen hinzugefügt, entfernt oder aktualisiert
- Die Identität (Name und E-Mail-Adresse) des Administrators, der die jeweilige Änderung vorgenommen hat
- Datum und Uhrzeit jeder Änderung

Die Prüfprotokolleinträge sind für die Rollen „Organisationsadministrator“ und „Administrator“ im Jamf Account zugänglich. Das Prüfprotokoll enthält eine vollständige Aufzeichnung aller Konfigurationsänderungen.

Datentyp	Aufbewahrungsfrist	Anmerkungen
Inhalt des Gesprächs	30 Tage	Automatisch gelöscht; kann nicht wiederhergestellt werden
Prüfprotokoll (Konfigurationsänderungen)	Standardmäßige Aufbewahrungsfrist für den Jamf Account	Zugänglich im Aktivitätsverlauf des Jamf Accounts
Kontext der Modellinferenz	Wird nach Ende der Sitzung nicht gespeichert	Wird bei Beendigung der Sitzung gelöscht
Modelltraining	Nicht zutreffend	Anthropic nutzt die Daten von AWS Bedrock nicht zum Training seiner Modelle.

Zugangskontrolle

Authentifizierung

Der KI-Assistent übernimmt die Jamf-Sitzung des authentifizierten Benutzers. Es sind keine separate Anmeldung, kein API-Schlüssel und keine Anmeldedaten erforderlich. Benutzer, die nicht in ihrer Jamf-Umgebung authentifiziert sind, können nicht auf den KI-Assistenten zugreifen.

Um den KI-Assistenten zu aktivieren, ist die Rolle „Administrator“ oder „Organisationsadministrator“ im Jamf Account erforderlich. Standardbenutzer und Benutzer mit Lesezugriff dürfen die Einstellungen der KI-Assistenten-Toolgruppe weder aktivieren noch deaktivieren oder ändern. Alle von Administratoren vorgenommenen Änderungen werden im Prüfprotokoll „Aktivitätsverlauf“ erfasst.

Autorisierung

Alle Tool-Abfragen werden mit den Berechtigungen des authentifizierten Benutzers ausgeführt. Der KI-Assistent erweitert keine Berechtigungen und umgeht keine bestehenden rollenbasierten Zugriffskontrollen von Jamf Pro:

- Abfragen zum Gerätebestand liefern nur Geräte, für deren Anzeige der Benutzer die Berechtigung besitzt
- Die Konfiguration berücksichtigt die bestehenden Zugriffskontrollen auf Objektebene bei der Auswertung der Ergebnisse
- Der Zugriff auf Konformitätsdaten erfolgt gemäß dem Standard-RBAC von Jamf Pro
- Ein Benutzer, der keinen Zugriff auf eine Richtlinie hat, kann die Details dieser Richtlinie auch nicht über den KI-Assistenten abrufen.

KI-Assistenten aktivieren und deaktivieren

Der KI-Assistent ist standardmäßig für alle Organisationen deaktiviert. Administratoren aktivieren diese Funktion explizit im Jamf Account unter „Organisation“ → „KI-Assistent“.

Das **Deaktivieren des KI-Assistenten** erfolgt umgehend und kann jederzeit rückgängig gemacht werden. Ein Administrator kann das Kontrollkästchen „KI-Assistent aktivieren“ ganz einfach im Jamf Account deaktivieren. Dadurch werden alle Funktionen des KI-Assistenten für alle Benutzer im gesamten Unternehmen sofort deaktiviert. Einzelne Werkzeuggruppen (Jamf Pro-Werkzeuge im schreibgeschützten Modus) können ebenfalls unabhängig voneinander deaktiviert werden, ohne den KI-Assistent-Kern zu deaktivieren.

Die Festlegung des **Anwendungsbereichs auf Umgebungsebene** bietet eine zusätzliche Kontrollebene für Organisationen, die eine vorsichtigere Einführung anstreben. Bei der Aktivierung der schreibgeschützten Tools von Jamf Pro können Administratoren den Zugriff auf bestimmte Umgebungen und Mandanten beschränken, anstatt sie für alle Umgebungen zu aktivieren. Auf diese Weise können Unternehmen den KI-Assistenten zunächst in einer Sandbox- oder Staging-Umgebung testen, bevor sie ihn im Produktivsystem aktivieren, ohne dass Änderungen an der Produktionsumgebung erforderlich sind.

Verfügbarkeit von Werkzeugen nach Produkt

Informationen zur aktuellen Verfügbarkeit der Tools, zu den Produktanforderungen und zum Betastatus werden im Jamf Learning Hub zur Verfügung gestellt.

Konformität

Der KI-Assistent wird im Rahmen des bestehenden Konformitätsprogramms von Jamf eingesetzt. Die aktuelle Liste der Jamf-Zertifizierungen finden Sie im Jamf Trust Center oder von Ihrem Account-Team.

AWS Bedrock-Konformität (gilt für die Inferenzebene):

- SOC 2 Typ II
- ISO 27001

FedRAMP und StateRAMP: Der KI-Assistent ist in StateRAMP- oder FedRAMP-zugelassenen Umgebungen nicht verfügbar. Wenden Sie sich an Ihr Jamf Account Team, um Einzelheiten zur Roadmap hinsichtlich der künftigen Verfügbarkeit von FedRAMP und StateRAMP zu erfahren.

Penetrationstest: Der KI-Assistent wurde im Rahmen des Sicherheitsüberprüfungsprogramms von Jamf einem Penetrationstest unterzogen. Die Ergebnisse stehen den Kunden auf Anfrage über Ihr Jamf Account Team unter Einhaltung einer Vertraulichkeitsvereinbarung zur Verfügung.

Zusammenfassung der Sicherheitsmaßnahmen

Kontrolle	Implementierung
Verschlüsselung während der Übertragung	TLS 1.2+ für die gesamte Kommunikation
Verschlüsselung der Daten im Ruhezustand	AWS KMS-Verschlüsselung
Authentifizierung	Übernimmt die Jamf Pro-Sitzung – keine separaten Anmeldedaten erforderlich
Rolle des Administrators erforderlich	Administrator oder Organisationsadministrator im Jamf Account
Autorisierung	Jamf Pro RBAC wird bei allen Tool-Abfragen durchgesetzt – keine Berechtigungserweiterung
Datenresidenz	Regionale Datenverarbeitung – USA/EU/APAC, keine regionenübergreifende Datenübermittlung
Datenzugriff durch Anthropic	Anthropic empfängt keine Kundendaten – die Inferenz erfolgt ausschließlich innerhalb von AWS Bedrock
Modelltraining	Es werden keine Kundendaten für das Modelltraining verwendet (AWS Bedrock)
Drittanbieter, die Daten verarbeiten	NowSecure (App-Risikoanalyse) – ausschließlich App-Identifikatoren; Apple GDMF (Betriebssystemversionen) — nur öffentliche Daten
Prüfprotokollierung	In der Aktivitätshistorie des Jamf Accounts protokollierte Konfigurationsänderungen – nach Benutzer, Aktion und Zeitstempel
Aufbewahrung der Gespräche	30 Tage
Schreibgeschützter Betrieb	Wird auf der Implementierungsebene durchgesetzt – alle Jamf Pro API-Aufrufe sind GET-Anfragen; im Tool-Code gibt es keine Schreibmethoden
Sitzungsisolierung	Die Konversationen sind auf den authentifizierten Benutzer und die Organisation beschränkt – andere Benutzer oder Organisationen haben keinen Zugriff darauf
Standardmäßig deaktiviert	Für alle Organisationen deaktiviert, bis dies von einem Administrator ausdrücklich aktiviert wird
Funktion deaktivieren	Sofort: Deaktivierung der Option „KI-Assistent aktivieren“ in Ihrem Jamf Account; diese Änderung kann jederzeit rückgängig gemacht werden
Umgebungsanalyse	Pro-Tools können auf bestimmte Umgebungen/Mandanten beschränkt werden, um einen kontrollierten Rollout zu gewährleisten
Web Application Firewall (WAF)	Wird auf der API-Gateway-Ebene in Produktiv- und Testumgebungen eingesetzt
„Guardrails“ von Bedrock	Inhaltsüberwachung über Schadenskategorien hinweg und Prompt-Injection-Erkennung bei hoher Sensitivität; alle Ereignisse werden rückverfolgt und protokolliert
Penetrationstests	Vor der Marktzulassung durchgeführt; Ergebnisse unter Geheimhaltungsvereinbarung verfügbar

Informationen zum Dokument

Veröffentlicht	April 2026
Verteilung:	Öffentlich
Standort	https://www.jamf.com/resources/technical-papers/ai-assistant-architecture-security/

Weitere Informationen

- **Jamf Trust Center** – Aktuelle Jamf-Zertifizierungen, Unterlagen zur Konformität und Sicherheitsstatus: https://www.jamf.com/de/trust-center/
- **Jamf Learning Hub** – Aktueller Katalog der KI-Assistenten-Tools, Produktanforderungen und Modellversion: https://learn.jamf.com/home
- **Dieses Dokument** – Die aktuellste Version dieses Dokuments finden Sie unter: jamf.it/aiassistant
- **Fragen?** Wenden Sie sich an Ihr Jamf Account Team.