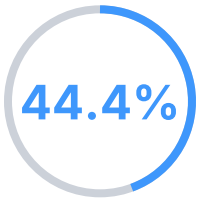
jamf

UMFRAGE VON JAMF ZUR KI-GOVERNANCE:

Erkenntnisse von 687 IT- und Sicherheitsverantwortlichen

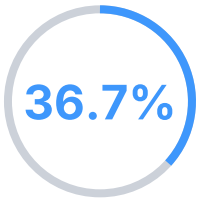
Zusammenfassung der Ergebnisse

687 IT- und Sicherheitsverantwortliche aus Apple-Unternehmen gaben Einblicke in den Umfang, die Ziele und die Sicherheit ihrer KI-Bereitstellung. Das haben wir herausgefunden.



Automatisierung

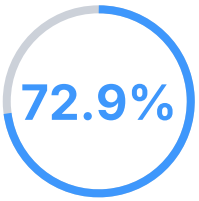
Bereitstellung



Kontrolle

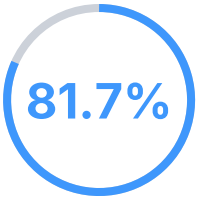
Drei Prioritäten im Bereich der KI laufen zusammen

Als oberste KI-Prioritäten nannten die Befragten die Automatisierung des IT-Betriebs (44,4 %), die Bereitstellung von KI-Produktivitätstools (41,0 %) und die Etablierung von KI-Governance (36,7 %).



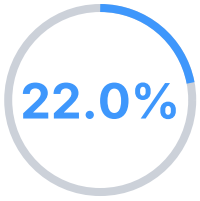
der Unternehmen nutzen KI

Fast drei Viertel der Unternehmen nutzen mittlerweile KI in irgendeiner Form. Es geht nicht mehr um das „Ob" der Einführung. Governance ist unumgänglich.



der Organisationen sind KI-Risiken ausgesetzt

22,0 % verzeichneten bereits einen Kosten- oder Sicherheitsvorfall. Weitere 59,7 % sehen darin ein kurzfristiges Risiko. Das KI-Risiko ist entweder bereits eingetreten oder wird zeitnah erwartet.



der Organisationen verzeichneten bereits einen Kosten- oder Sicherheitsvorfall

Mehr als jedes fünfte Unternehmen erlitt bereits Kosten- oder Sicherheitsvorfälle. Die Auswirkungen betreffen sowohl das Budget als auch das Sicherheitsteam.

Anstieg der Inzidenzrate

Unter den Unternehmen, in denen KI bereits umfassend in die Geschäftsprozesse integriert ist, verzeichneten 27,1 % einen KI-bezogenen Vorfall, verglichen mit 19,4 % derjenigen, die sich noch in der Sondierungsphase befinden. Das Sicherheitsrisiko skaliert mit dem Grad der Einführung, nicht umgekehrt.

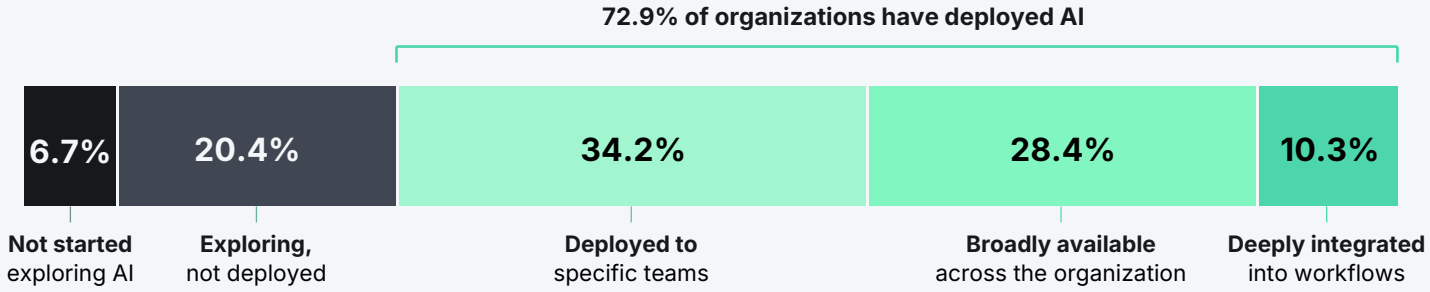
Je intensiver Sie KI nutzen, desto größer ist Ihr Risiko.

Die meisten Unternehmen forcieren die Einführung von KI, doch damit steigen auch die Risiken. Schatten-KI, unauffällig integrierte Softwarefunktionen sowie Geräte- und agentenbasierte Tools schaffen blinde Flecken, die schwer zu kontrollieren und noch schwerer zu prüfen sind. Je weiter sich die Nutzung verbreitet, desto größer wird auch das Risiko. Und dann ist die Frage nicht mehr, ob es zu einem Vorfall kommen wird, sondern wann.

ABBILDUNG 1

Wo Apple-Unternehmen bei der Einführung von KI stehen

Das Wichtigste auf einen Blick: Fast drei Viertel der Apple-Unternehmen nutzen mittlerweile KI in irgendeiner Form, von Pilotprojekten auf Teamebene bis hin zur tiefgreifenden Integration in die täglichen Arbeitsabläufe. Die Entscheidung über die Einführung ist bereits gefallen.



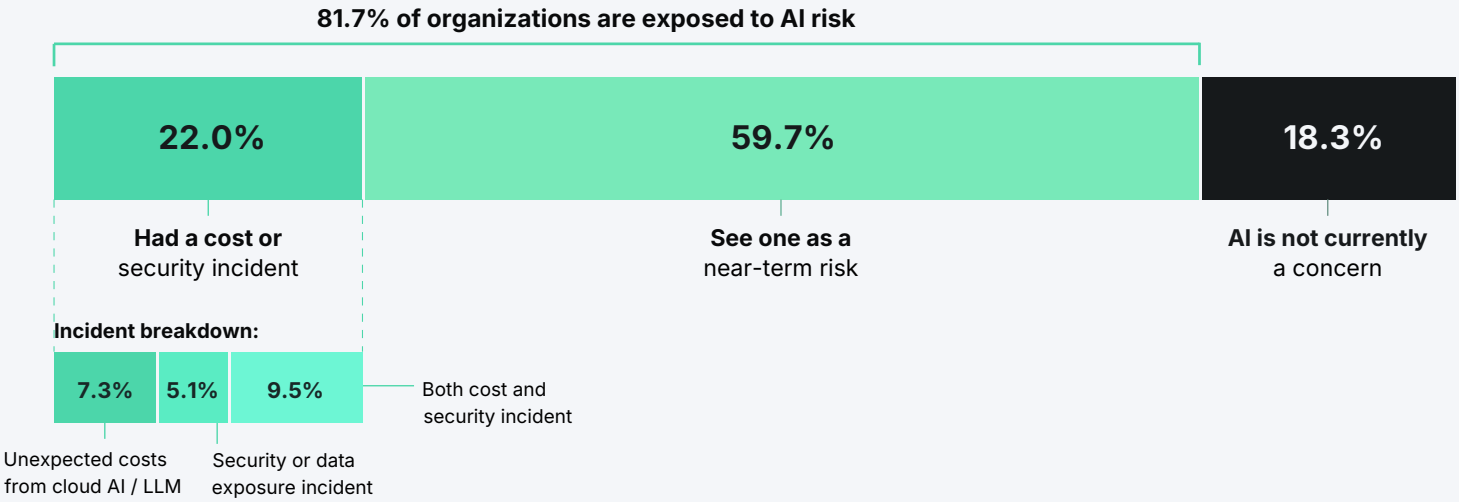
Anmerkung: n = 687 Führungskräfte aus den Bereichen IT und Sicherheit. Q2/ 2026.

Auch wenn fast drei von vier Unternehmen KI einsetzen, führt die unternehmensweite Bereitstellung keineswegs zu einer Verringerung des Risikos. Ganz im Gegenteil, es verschärft die Situation noch. 22,0 % erlebten bereits Vorfälle: 7,3 % durch unerwartete Cloud-KI- oder LLM-Kosten, 5,1 % durch Sicherheits- oder Datenlecks und 9,5 % durch beides. Bei denjenigen, die noch keinen Vorfall verzeichnet haben, rechnen 59,7 % damit.

ABBILDUNG 2

Vorfälle und Bedenken im Zusammenhang mit KI in den letzten 12 Monaten

Das Wichtigste auf einen Blick: 22,0 % der Unternehmen erlebten bereits einen KI-bezogenen Vorfall. Weitere 59,7 % rechnen damit. Nur 18,3 % geben an, dass KI derzeit kein Thema für sie ist.



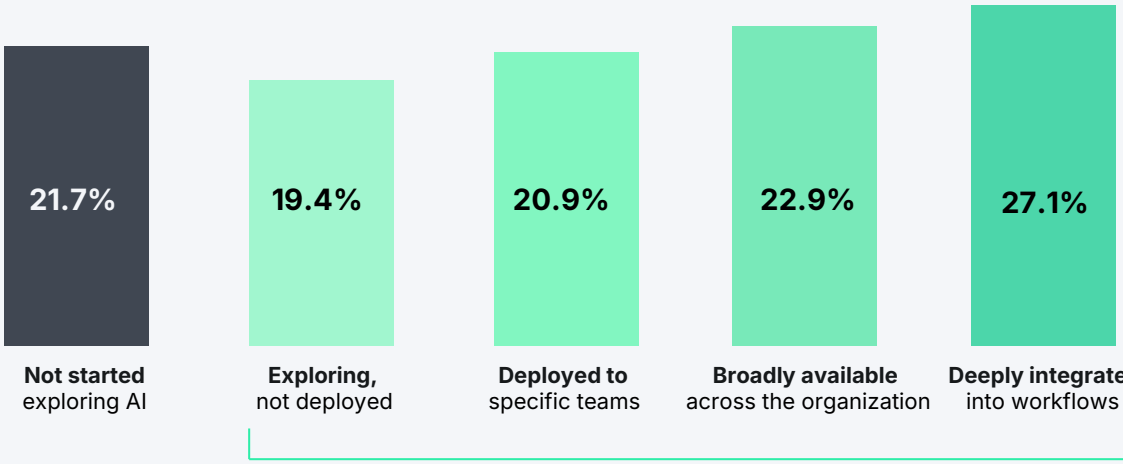
Fußnote: *n = 681. Dieses Muster zeigt sich unabhängig voneinander in beiden Stichproben.*

Die Daten liefern jedoch ein überraschendes Ergebnis: Die Unternehmen, die bei der KI am weitesten fortgeschritten sind, melden die meisten Vorfälle.

ABBILDUNG 3

KI-Vorfälle nach Tiefe der Implementierung

Das Wichtigste auf einen Blick: Apple-Unternehmen, die KI weitreichend einsetzen, melden häufiger Vorfälle. Bei den am weitesten fortgeschrittenen Benutzern erlebten bereits 27,1 % einen Vorfall, verglichen mit 19,4 %, die sich noch in der Testphase befinden.



Anmerkung: n = 683 Führungskräfte aus den Bereichen IT und Sicherheit. Q2/ 2026

Sobald Teams beginnen, sich in ihrem Unternehmen mit KI zu befassen, steigt die Wahrscheinlichkeit, dass es zu einem Vorfall kommt. Der Anteil der Unternehmen, die einen Vorfall verzeichneten, ist bei denjenigen mit einer umfassenden Integration von KI (27,1 %) um 40 % höher als bei denjenigen, die sich noch in der Sondierungsphase befinden (19,4 %).

⚠ Typische Muster bei KI-Herausforderungen

Die Freitextantworten der Befragten zur Vorbeugung von Vorfällen konzentrierten sich auf vier Themenbereiche.

Schatten-KI

Produktivitätssteigerungen, ein Boom bei KI-Tools und unternehmensweite Bemühungen um die Integration von KI führen dazu, dass Mitarbeiter regelmäßig auf KI zurückgreifen. Dies geschieht oft ohne Genehmigung der IT-Abteilung; Mitarbeiter richten persönliche Accounts ein und geben unter Umständen sensible Daten weiter. Infolgedessen weiß die IT-Abteilung nicht, welche KI-Systeme zum Einsatz kommen, was es schwierig macht, KI-Plattformen zu kontrollieren oder zu blockieren. Fehlende Sichtbarkeit macht Sicherheit und Governance nahezu unmöglich.

Anbieterflut

Abgesehen von der Flut neuer KI-basierter Software integrieren viele Apps bereits KI in ihre bestehenden Produkte. Die Prüfung und Bereitstellung jedes einzelnen KI-Tools ist für IT-Teams zeitaufwendig und schwierig, insbesondere angesichts des rasanten Tempos, mit dem sich KI weiterentwickelt. Die Befragten geben an, dass es ihnen schwerfällt, zu entscheiden, welche KI-Plattformen für ihre Mitarbeiter am besten geeignet sind, und die Mitarbeiter dazu zu bewegen, die genehmigten KI-Tools zu nutzen. Diese zunehmenden Angriffspunkte erschweren die Absicherung von KI.

Agentische KI und KI für Entwickler

Herausforderungen bei der im Zusammenhang mit agentischer KI und KI für Entwickler zeigen sich in einigen Schlüsselbereichen: sichere Bereitstellung/Transparenz, KI-Funktionen und Schulung der Benutzer. Laut der Befragten ist die sichere Bereitstellung agentischer KI bei gleichzeitigem Datenschutz eine Kernherausforderung. Außerdem treten häufig Probleme mit der Transparenz bei Befehlszeilentools, Paketen von Drittanbietern, IDE-Erweiterungen, eingebetteten LLMs und vielem mehr auf. Sofern die entsprechenden Berechtigungen erteilt wurden, birgt agentische KI erhebliche Risiken für Codebasen, wenn unsicherer oder problematischer Code hinzugefügt oder notwendiger Code entfernt wird. Entwicklungsprobleme betreffen auch Benutzer, die selbst keine Entwickler sind, da sie ihre eigenen Apps ohne angemessene Prüfung und Qualitätskontrolle entwickeln.

Unerwartete Kosten

Der Spagat zwischen Kosten, Unternehmensinitiativen und Sicherheitsanforderungen stellt IT-Teams vor große Herausforderungen. Die nutzungsbasierte Abrechnung für Cloud-KI- und LLM-APIs erschwert die Ausgabenprognose, und da Abteilungen rasch neue Tools einführen, häufen sich redundante kostenpflichtige Lizenzen an. Ohne Einblick in die tatsächliche Nutzung haben IT-Teams keine klare Grundlage, um zu entscheiden, welche Tools konsolidiert werden können.

Governance und Produktivität gehen Hand in Hand.

Unter den KI-Benutzern gilt: Je tiefer KI integriert ist, desto höher ist die Vorfallsrate.

Typische Herausforderungen der Befragten sind Transparenz, Bereitstellung, Anbieterflut und Kosten.

Zusammengenommen machen diese Erkenntnisse eines deutlich: **KI wird schneller eingeführt, als sie reguliert werden kann.**

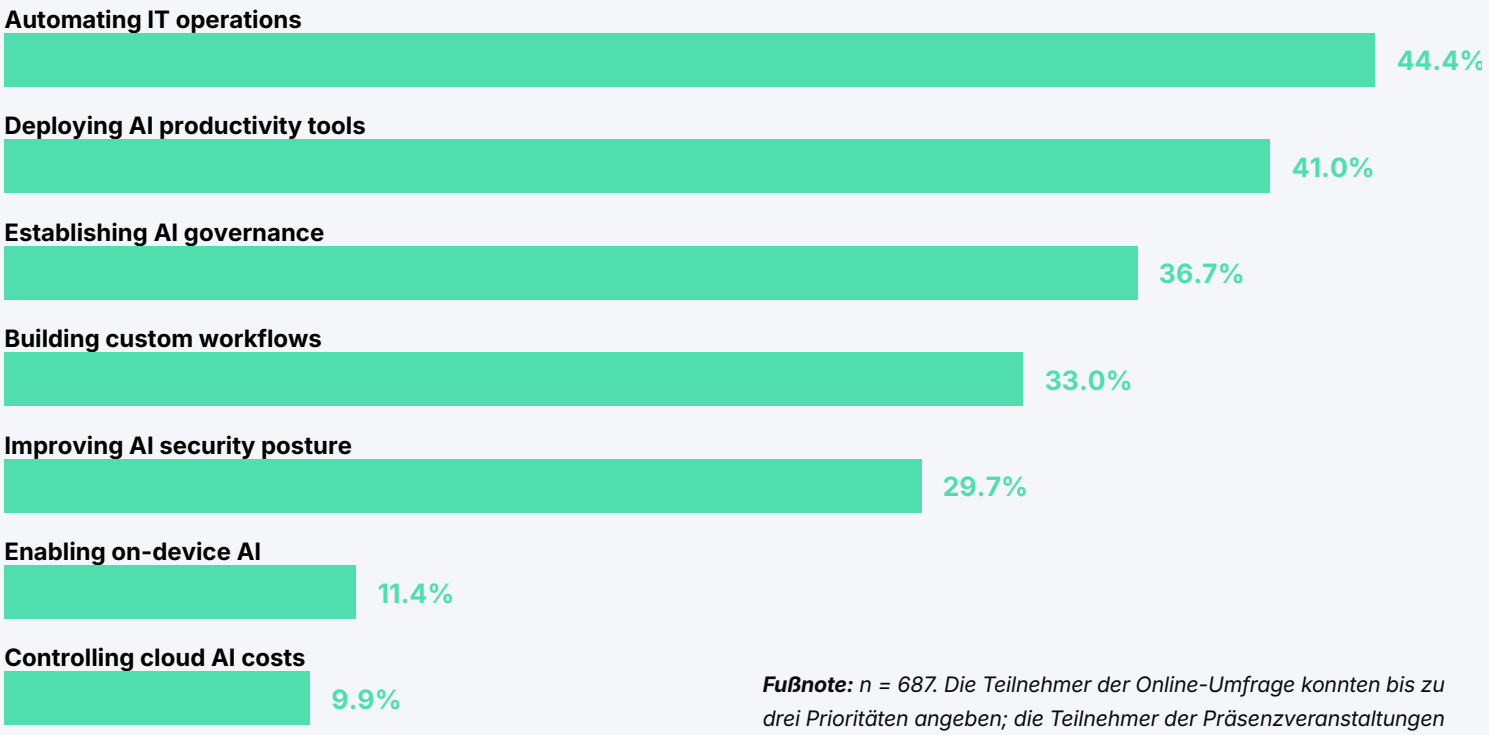
Dies äußert sich in einer „Schatten-KI", ungeschützten Zugriff auf Unternehmensdaten oder -systeme, der Einführung redundanter (und kostspieliger) Plattformen sowie Risiken, die schwer zu messen sind, da die IT-Abteilung nichts davon mitbekommt.

Als Reaktion darauf müssen IT-Teams ihre Prioritäten überdenken, da KI die Arbeitsweise aller Beteiligten grundlegend verändert.

ABBILDUNG 4

Die Prioritäten in Bezug auf KI für die nächsten 12 Monate

Das Wichtigste auf einen Blick: Die Automatisierung des IT-Betriebs, die Bereitstellung von Tools für produktives Arbeiten und die Etablierung von Governance-Strukturen werden in ähnlichem Umfang vorangetrieben. Governance läuft nicht hinter der Befähigung her, sondern hält mit ihr Schritt.



Fußnote: *n = 687. Die Teilnehmer der Online-Umfrage konnten bis zu drei Prioritäten angeben; die Teilnehmer der Präsenzveranstaltungen wählten eine aus. Weitere Einzelheiten finden Sie in der Methodik.*

Governance und Enablement wirken oft wie Gegensätze. Je mehr KI-Tools es gibt, desto schwieriger ist es, sie zu kontrollieren. IT-Teams mussten schon immer konkurrierende Prioritäten ausbalancieren – KI bildet hier keine Ausnahme. Das Tempo der KI-Bereitstellung ist rasant; ihre Funktionen und Risiken dringen in Neuland vor.

Deshalb verfolgen die Teams diese Prioritäten gleichzeitig. Wenn man zu schnell ist, erhöht sich die Wahrscheinlichkeit eines Vorfalls. Wenn man zu langsam ist, suchen die Mitarbeiter nach alternativen Möglichkeiten, die Ihre Sicherheitslage beeinträchtigen.

💬 KI-Herausforderungen im Branchenvergleich

178 offene Antworten lieferten tiefe Einblicke zur Einordnung der Ergebnisse. Acht Antworten, die wir erhalten haben*:

Die Benutzer wollen sofortigen Zugriff, und die Sicherheitsteams, die dies blockieren, stehen unter Druck. Das Kernproblem besteht weiterhin: **Eine lückenlose Kontrolle beeinträchtigt tendenziell die Produktivität, doch eine Lockerung der Kontrollen gefährdet die Konformität.**

Jeder Anbieter integriert KI, ob man das will oder nicht. Das pauschale Deaktivieren verschafft zwar Zeit, ist aber keine Dauerlösung. Die größere Sorge ist, wie die Daten in der Cloud verarbeitet werden und ob wir kontrollieren können, wohin unsere Daten gehen.

Bekannte KI-Websites zu blockieren, ist einfach. CLI-Tools, IDE- und Browser-Erweiterungen sowie GitHub-Pakete **sind weitgehend unsichtbar**; wird ein Vektor geschlossen, weichen Benutzer auf einen anderen aus.

In regulierten Branchen und bestimmten Rechtsräumen müssen spezifische Rahmenbedingungen für die Konformität vorhanden sein, bevor überhaupt etwas in Betrieb genommen werden kann, und derzeit **erfüllen die Tools und Rahmenbedingungen diese Anforderungen nicht.**

Schatten-KI und Black-Box-Skriptausführung sind die Top-Risiken. Dicht dahinter folgen nicht-technisch versierte Benutzer, die ihre eigenen Apps programmieren, Dinge entwickeln, die sie nicht vollständig verstehen, und dabei Daten preisgeben, ohne sich dessen bewusst zu sein.

Es besteht eine Diskrepanz zwischen der Erwartungshaltung, dass jeder KI nutzt, und der Bereitschaft, die Lizenzen zu finanzieren. Teams, die schnell gehandelt haben, haben nun mehrere überlappende Agenten, **hohe Kosten und kein Framework** zur Konsolidierung der Tools.

Freigaben für KI-Agenten auf Entwicklungs- und Produktionsumgebungen stoßen auf großen Widerstand. Es besteht die Angst, das ein Agent unerwünschte Aktionen ausführt und danach den totalen Datenverlust meldet. **Die kontrollierte und gesteuerte Bereitstellung agentischer Fähigkeiten ist nach wie vor ein ungelöstes Problem.**

Und wenn halluzinierte Ergebnisse als Fakten behandelt werden und sich KI immer tiefer in unseren Alltag einbettet, **nehmen die Risiken schneller zu als die Kompetenz im Umgang damit.**

* Die oben genannten Themen wurden von Jamf basierend auf Mustern aus 178 Freitextantworten formuliert. Jede spiegelt ein wiederkehrendes Thema wider, nicht den genauen Wortlaut einzelner Befragter.

Strategische Umsetzung: vier Governance-Grundsätze

1.

Mehr Transparenz

Viele Befragte erklärten, dass es von entscheidender Bedeutung ist, Transparenz zu schaffen. Man kann nicht kontrollieren, was man nicht sieht. Doch genau darin liegt die Schwierigkeit. Regelmäßige Überprüfungen der installierten Apps und die Überwachung des Datenverkehrs tragen dazu bei, Interaktionen mit KI-Plattformen zu erkennen. Die Nutzung lokaler KI-Plattformen sowie KI-Erweiterungen in freigegebenen Apps erfordern eine intensivere Analyse der KI-Laufzeitüberwachung.

2.

Das Tool kontrollieren, nicht den Benutzer

In vielen Unternehmen wurden die KI-Richtlinien schnell und ohne Rücksprache mit der IT-Abteilung eingeführt. Und diese Maßnahmen fördern einen verstärkten Einsatz von KI – und zwar so schnell wie möglich. Selbst wenn den Benutzern Anleitungen zur Verfügung gestellt werden, sind diese keine verbindlichen Vorschriften. Und dann wird Schatten-KI genutzt.

Stattdessen wäre es besser, wenn die Governance basierend auf der Risikotoleranz und den Sicherheitsrichtlinien des Unternehmens festgelegt und in den Datenfreigabe-Einstellungen des KI-Tools abgebildet werden: worauf es zugreift, wie es Daten verarbeitet und was es ändern darf. Bei der Schatten-KI ist der Benutzer nicht immer sichtbar, wohl aber der Datenverkehr, die Daten und die API-Aufrufe. Man kann nur das kontrollieren, was man sieht.

3.

Governance als festen Bestandteil der Bereitstellung etablieren

Organisationen, die KI übereilt implementierten, gingen potenzielle Sicherheitsrisiken ein. Die Reihenfolge ist entscheidend – die Governance muss die Bereitstellung von Apps aktiv begleiten und darf nicht nur darauf reagieren. Ja, das ist leichter gesagt als getan, und vielleicht haben Sie bereits einen Rückstand aufzuholen. Die Identifikation genutzter Tools, deren Bereitstellung und klare Zugriffskritierien erleichtern die sichere KI-Skalierung.

4.

Nutzen Sie nativ für Apple entwickelte Tools statt nachträglich angepasster Lösungen.

Netzwerkbasierte Tools zeigen Ihnen den Datenverkehr an: welche Cloud-KI-Dienste die Benutzer wann und wie oft aufrufen. Das ist zwar ein echtes Signal, aber es endet am Rand des Netzwerks. Selbst wenn die KI selbst in der Cloud ausgeführt wird, erfolgt der Zugriff auf dem Gerät: welche Tools installiert sind, welche Prozesse sie starten und auf welche Dateien sie zugreifen. Nichts davon taucht in einem DNS-Protokoll auf. Apple-nativeTools schließen diese Lücke: Zeigen Sie die Tools, die Prozesse und den Dateizugriff an und legen Sie fest, welche davon zulässig sind.

Regulieren, was Sie zulassen. Freigeben, was Sie kontrollieren.

KI entwickelt sich schneller, als die meisten Governance-Frameworks bewältigen können. Bisherige Herausforderungen müssen Ihre künftige Bereitstellungsstrategie nicht negativ beeinflussen. Man muss sich nicht entscheiden zwischen der Bereitstellung der benötigten KI-Tools für die Benutzer und der Gewährleistung einer sicheren Nutzung dieser Tools.

Erfolgreiche Teams setzen nicht auf maximale Geschwindigkeit oder totale Blockade. Sie betrachten Governance und Enablement als ein und dasselbe Projekt und integrieren von Anfang an Transparenz und Zugriffskontrollen in die KI-Bereitstellung. Für Apple-Unternehmen hängt dies von Werkzeugen ab, die die verwaltete Laufzeit kennen: Cloud-Datenverkehr, lokale Modelle und agentische Prozesse senden spezifische Signale, die ein nicht für Apple optimiertes Monitoring kaum erfasst. Die von Ihnen aufgebaute Governance ist nur so stark wie das, was Ihre Tools erkennen können.

Die Einführung von KI lässt sich nicht aufhalten. Aber man kann es in den Griff bekommen – und genau da fängt die Arbeit an.

Methodik

Die Daten wurden in zwei Phasen erhoben. Phase eins erfolgte im März und April 2026 in der Community der Kunden von Jamf (338 Befragte). Die zweite Runde war eine persönliche Befragung auf den Jamf Nation Live-Veranstaltungen in sechs nordamerikanischen Städten (349 Befragte). Gesamtzahl der Befragten: 687 Führungskräfte aus den Bereichen IT und Sicherheit. Alle Befragten arbeiten in Unternehmen, die als Kunden von Jamf Apple-Geräte in großem Umfang verwalten und schützen.

Bei der Frage nach den Prioritäten sollten die Befragten ihre wichtigsten KI-Prioritäten für die nächsten 12 Monate auswählen. Bei den Umfragen im März und April waren bis zu drei Antworten möglich; bei der Jamf Nation Live-Umfrage war nur eine Antwort möglich. Die Prozentangaben zu dieser Frage geben den Anteil aller 687 Befragten wieder, die die jeweilige Priorität unter ihren wichtigsten Auswahlmöglichkeiten genannt haben. Aus Gründen der Transparenz werden hier beide Auswahlkriterien offengelegt.

Statistische Auswertungen bestätigen, dass die beiden Erhebungsrunden unterschiedliche Gruppen ergaben, wobei die Befragten von Jamf Nation Live im Durchschnitt einen früheren Reifegrad im Bereich KI aufwiesen. Die Tendenzergebnisse gelten unabhängig voneinander für beide Stichproben. Alle Daten der Befragten wurden anonymisiert erhoben und ausgewertet; einzelne Antworten werden keinen bestimmten Befragten oder Organisationen zugeordnet. Die Befragten erhielten für ihre Teilnahme keine Vergütung.