netskope

Sichere KI: Crucial Conversations – Fünf entscheidende Gespräche für CISOs

Inhalt

Einleitung: Ein zweischneidiges Mandat für die KI

Aufgrund der entscheidenden Rolle, die Technologie heute in modernen Unternehmen spielt, rückt die IT-Abteilung stärker denn je in den Fokus. Infolgedessen suchen IT-Führungskräfte in einer Reihe entscheidender Gespräche mit ihrem CEO, dem Vorstand und anderen Führungskräften nach Wegen, um Technologien zur Steigerung des Unternehmenserfolgs einzusetzen. Dabei spielt kein Thema eine größere Rolle als die künstliche Intelligenz.

KI stellt für CIOs, CISOs und ihre Teams eine besondere Herausforderung dar. Im Netskope-Bericht „Crucial Conversations“[1] haben wir aufgezeigt, dass CEOs ihren IT-Führungskräften ein zweischneidiges Mandat erteilen: Sie sollen KI integrieren, um deren experimentelle Nutzung zu fördern und einen messbaren Geschäftswert zu erzielen. Gleichzeitig sollen sie jedoch auch die Kosten reduzieren, als Gatekeeper gegen überhöhte Ausgaben fungieren, übertriebene Erwartungen dämpfen und vor potenziellen Datenlecks oder Sicherheitsverletzungen schützen.

Kurz gesagt: IT-Führungskräfte müssen die KI nutzen, um disruptiven Innovationen den Weg zu ebnen, und das Unternehmen gleichzeitig vor den damit verbundenen Risiken schützen. Diese Doppelaufgabe setzt das Personal massiv unter Druck.

Jedes Unternehmen befindet sich in einer anderen Phase der KI-Reife. Einige versuchen immer noch, Anwendungsfälle für den sinnvollen Einsatz von KI zu finden, während andere bereits mit Hochdruck an der Entwicklung eigener KI-Anwendungen arbeiten und ihre Mitarbeiter zur intensiven Nutzung dieser Tools anhalten. Alle versuchen, KI als Wachstumsmotor zu nutzen, doch jeder hat andere Ausgangsbedingungen und schreitet in unterschiedlichem Tempo voran.

[1] https://www.netskope.com/crucial-conversations

Fünf Schritte zu einer erfolgreichen KI-Einführung

Unabhängig vom KI-Reifegrad Ihres Unternehmens müssen Sie einige wichtige Sicherheitsaspekte berücksichtigen. Entscheidend ist, sich bei der Planung einer Sicherheitsstrategie der mit jeder Phase verbundenen Risiken voll bewusst zu sein.

1. **Können wir mit KI-Tools** experimentieren und gleichzeitig die Risiken der Schatten-KI effektiv managen?
2. **Sind wir in der Lage, in SaaS-Plattformen** integrierte KI zu nutzen, ohne dass dabei unbefugt Daten ausgetauscht werden?
3. **Wie können wir eigenständige KI-Anwendungen** verwalten und Datenlecks verhindern?
4. Wie können wir bei der **Entwicklung privater KI-Anwendungen** schädliche oder verzerrte Modellausgaben und häufig auftretende Anwendungsschwachstellen verhindern?
5. Wie können wir bei der **Bereitstellung autonomer Agenten verhindern, dass ihnen zu weitreichende Zugriffsrechte gewährt werden**?

Experimentieren

In SaaS-Plattformen integrierte KI

Zugelassene eigenständige KI-Apps

Private KI-Anwendungen

Autonome Agenten

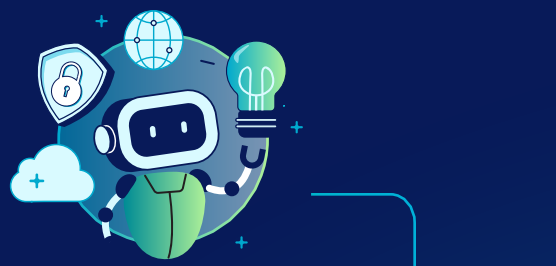
Produktivere Gespräche auf Führungsebene

KI ist heute nicht nur das Hauptgesprächsthema unter Technologieexperten, sondern auch eine der wichtigsten Prioritäten in den Führungs- und Vorstandsetagen. Durch unsere Umfrage unter CEOs[1] wissen wir, dass sie vom Potenzial der KI begeistert sind und von ihren IT-Führungskräften eine Strategie zur Einführung und Integration dieser Technologie erwarten – jedoch ohne sich von dem in der Branche grassierenden Hype blenden zu lassen.

IT-Fachkräfte, vor allem im Sicherheitsbereich, müssen KI so einzusetzen, dass keine Kompromisse bei der Leistung und Sicherheit eingegangen werden, die Einhaltung gesetzlicher Vorschriften aber gewährleistet bleibt. Gleichzeitig sollen die Kosten gesenkt und die Komplexität reduziert werden. Wenn die Implementierungspläne detaillierter werden, müssen sie die damit verbundenen geschäftlichen Vorteile und Risiken stets im Auge behalten.

Wir hoffen, mit diesem E-Book einen Beitrag zum Erreichen dieser Ziele zu leisten. ***Sichere KI: Crucial Conversations – Fünf entscheidende Gespräche für CISOs*** soll Sicherheitsteams dabei helfen, ihre KI-Projekte mit Zuversicht anzugehen und produktivere Gespräche über die Herausforderungen und Chancen der KI zu führen. Das E-Book soll Unternehmen insbesondere dabei unterstützen, KI-fähige Grundsätze in ihre Sicherheitsstrategie einzubinden und Sicherheitsgrundsätze in ihre KI-Strategie zu integrieren, damit Sicherheit zu einem Wachstumsmotor und nicht zu einem Hemmschuh wird.

[1] *https://www.netskope.com/crucial-conversations*



Disruption durch KI, Abwehr von Risiken – drei Grundsätze, die priorisiert werden müssen.

Ganz gleich, an welchem Punkt Ihrer KI-Einführung Sie sich gerade befinden: Es gilt, drei wichtige Grundsätze zu beachten, um das Potenzial dieser Technologie auf sichere Weise auszuschöpfen.

1. **Transparenz:** Sicherheitsteams benötigen einen umfassenden Überblick über ihre KI-Landschaft, um zu wissen, welche KI-Tools auf welche Weise eingesetzt werden.

2. **Schutz:** Sicherheitstechniker müssen kontextbezogene Schutzmaßnahmen umsetzen, damit das Unternehmen durch dynamische, anpassungsfähige Sicherheitsmechanismen geschützt wird, ohne Innovationen auszubremsen.

3. **Reife:** Durch die proaktive Analyse ihrer Daten und Anwendungen können Sicherheitsexperten eine KI-Reife erreichen, die ihr Unternehmen auf Erfolgskurs bringt.

Schritt 1: Experimentieren

Können wir mit KI-Tools experimentieren und gleichzeitig die Risiken der Schatten-KI eindämmen?

Als ChatGPT im November 2022 eingeführt wurde, eroberte es die Welt im Sturm – und sorgte bei Unternehmen für große Überraschung. Innerhalb kürzester Zeit begannen Mitarbeiter, private Versionen von KI-Chatbots zu nutzen, um ihre Arbeitsaufgaben schneller zu erledigen oder Probleme zu lösen. Die Schatten-KI stellt auch heute noch für viele Unternehmen ein Problem dar: Laut einer Studie von Netskope Threat Labs[1] nutzen im Jahr 2025 immer noch erstaunliche 72 % aller Unternehmensnutzer private Konten, um am Arbeitsplatz auf ChatGPT, Google Gemini und andere beliebte GenAI-Anwendungen zuzugreifen.

Dieses Problem verschärft sich immer mehr. Fast alle gängigen SaaS-Anwendungen verfügen mittlerweile über integrierte KI-Funktionen; KI-Modelle kommunizieren heute direkt miteinander; Agenten können mithilfe natürlicher Sprache erstellt werden und sind somit nicht mehr nur technisch versierten Anwendern vorbehalten. Und all diese KI-Instanzen interagieren mit mehr Daten und Anwendungen, als es für Menschen jemals möglich wäre. Infolgedessen breitet sich die Schatten-KI in einem noch nie dagewesenen Tempo aus.

72 % aller Unternehmensnutzer verwenden bei der Arbeit weiterhin ihre privaten Konten, um auf GenAI-Anwendungen zuzugreifen.

Netskope, Generative AI Cloud and Threat Report 2025

[1] https://www.netskope.com/resources/reports-guides/cloud-and-threat-report-generative-ai-2025

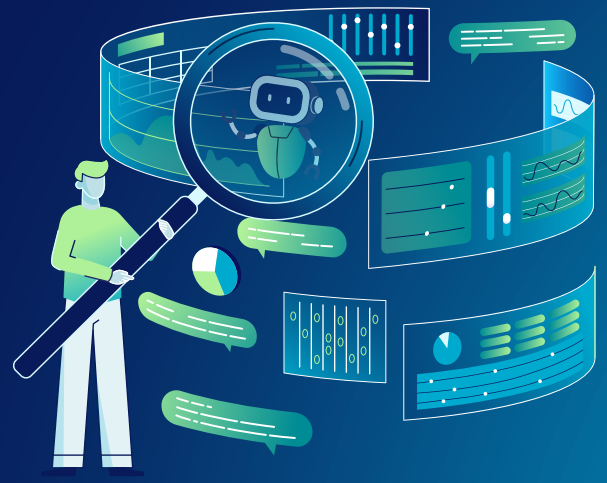
Derartig umfangreiche und detaillierte Einblicke in die KI-Landschaft sind für Sicherheitsteams unerlässlich. Sie brauchen Transparenz über alle in ihrem Unternehmen eingesetzten KI-Tools, inklusive nicht verwalteter Anwendungen und privater Instanzen. Außerdem benötigen sie fundierte Einblicke, um zu verstehen, was Benutzer und Agenten bei diesen Interaktionen tatsächlich tun.

Nur mit diesem Grad der Transparenz können Sicherheitsteams strategische Kontrolle über die KI-Aktivitäten in ihrem Unternehmen erlangen, anstatt sich blind darauf zu verlassen, dass alles in Ordnung ist.

Die harsche Realität ist, dass man nur das schützen kann, was man auch sieht.

Unser Ansatz

Mit Netskope One Cloud Access Security Broker (CASB) und Next Generation Secure Web Gateway (NG-SWG) erhalten Unternehmen einen detaillierten Überblick über die in ihrer Umgebung stattfindenden KI-Aktivitäten. Unser KI-Dashboard liefert ausführliche Informationen über alle Benutzeraktivitäten, etwa welche Benutzer auf welche Anwendungen zugreifen und welche Aktionen sie dabei ausführen. Es unterstützt Unternehmen bei der laufenden Erkennung und Überprüfung sämtlicher öffentlicher LLM-Interaktionen (Daten während der Übertragung), einschließlich der Interaktionen zwischen Benutzern und Anwendungen.



Schritt 2: In SaaS-Plattformen eingebettete KI

Sind wir in der Lage, in SaaS-Plattformen integrierte KI zu nutzen, ohne dass dabei unbefugt Daten ausgetauscht werden?

LLMs und spezielle KI-Anwendungen sind im Hinblick auf KI nicht mehr die einzigen Risikofaktoren. Je mehr sich die Technologie weiterentwickelt, desto häufiger werden KI-Funktionen in SaaS-Anwendungen integriert – von Videotelefonie-Plattformen über Tools zur Produktivitätssteigerung bis hin zu Vertriebsmanagementsystemen.

Diese SaaS-Tools sind oft eng in die Prozesse moderner Unternehmen eingebunden: Sie werden täglich für wichtige Geschäftsabläufe benötigt und können daher kaum gesperrt oder entfernt werden. Außerdem steigern KI-Funktionen die Produktivität oft so erheblich, dass kein Unternehmen darauf verzichten möchte.

Neue KI-Funktionen lassen sich meist mit minimalem Aufwand integrieren, unter anderem als Teil eines allgemeinen Updates, wobei nur sehr wenige Informationen zu den Nutzungsbedingungen für die Daten bereitgestellt werden. Bei einer Videotelefonie-Anwendung könnte zum Beispiel automatisch ein KI-Notizenprogramm aktiviert werden, das vertrauliche Unternehmensdaten aufzeichnet und speichert. Das ist etwas, dessen sich Sicherheitsteams oft nicht bewusst sind.

Eine bestehende SaaS-Anwendung kann mit neuen KI-Funktionen ausgestattet werden und diese sogar automatisch freischalten. Auch das kann ohne das Wissen des Sicherheitsteams geschehen.

Sicherheitsexperten benötigen einen umfassenden Überblick über ihre SaaS-Anwendungen. Sie müssen wissen, welche KI-Funktionen diese bieten, wie sie funktionieren und welche vertraglichen Bestimmungen für die Daten-Governance gelten. Sie müssen verstehen, wie jede Anwendung KI nutzt, ob sie Ihre Daten zum Trainieren ihrer Modelle verwendet, ob alle wichtigen Vorschriften eingehalten werden und ob sich die KI-Funktionen deaktivieren lassen.

Unternehmen sollten unbedingt die Kategorisierung und Klassifizierung sensibler Daten in Erwägung ziehen, damit sie gezielte Richtlinien zum Schutz ihres geistigen Eigentums oder ihrer regulierten Daten durchsetzen können. Für andere, nicht vertrauliche Informationen können dann weniger strenge Regeln angewandt werden.

Unser Ansatz

Der Cloud Confidence Index (CCI) von Netskope ist eine Datenbank mit über 85.000 SaaS-Anwendungen, die umfassende Informationen zu den damit verbundenen Risiken liefert. Anhand dieser Informationen können Sicherheitsteams fundierte Entscheidungen darüber treffen, welche KI-gestützten Anwendungen zugelassen, eingeschränkt oder gesperrt werden sollten.

Schritt 3: Verwaltete eigenständige KI-Anwendungen

Wie können wir eigenständige KI-Anwendungen verwalten und Datenlecks verhindern?

Mittlerweile haben sich viele Unternehmen für ein bestimmtes KI-Tool entschieden, zum Beispiel ChatGPT von OpenAI, Copilot von Microsoft, Gemini von Google oder Claude von Anthropic. Die Nutzung eines einzigen Systems für das gesamte Unternehmen bietet offensichtliche Vorteile in Bezug auf unternehmensgerechte Funktionen, verbesserte Lernmöglichkeiten und einheitliche Sicherheitsmechanismen. Wenn das Unternehmen dann noch andere KI-Systeme blockiert, verringert sich auch die potenzielle Angriffsfläche erheblich.

Durch diesen Ansatz werden Risiken jedoch nicht vollständig beseitigt. Ein unternehmenseigenes KI-Tool entfaltet seinen wahren Wert erst dann, wenn es mit anderen Dokumenten und Informationsquellen im Unternehmen verbunden wird. Dies würde bestimmten Benutzern jedoch die Möglichkeit geben, Daten aus internen Dokumenten abzurufen, auf die sie eigentlich keinen Zugriff haben sollten – was wiederum zu einem Datenleck im Unternehmen führen könnte.

Dadurch kann zum Beispiel verhindert werden, dass Mitarbeiter aus der Marketingabteilung eine mit übermäßigen Berechtigungen ausgestattete Unternehmens-KI nach neuen Features in der Produkt-Roadmap fragen und dann Informationen aus vertraulichen Dokumenten bekommen, auf die sie eigentlich keinen Zugriff haben sollten.

Unser Ansatz

Netskope schützt aktiv vor KI-spezifischen Bedrohungen zur Laufzeit. Sobald ein Benutzer versucht, vertrauliche Daten einzugeben, greift die Data Loss Prevention (DLP) von Netskope One automatisch ein und verhindert, dass personenbezogene Daten, Quellcode oder Geschäftsgeheimnisse in das KI-Modell gelangen. Dabei kann auch ein Popup-Fenster mit Coaching-Informationen für den Benutzer ausgelöst werden.

Gleichzeitig sorgt Netskope One AI Guardrails bei jeder Interaktion für eine Inhaltsmoderation in Echtzeit. Die Absicht hinter Prompts und Antworten wird analysiert, um raffinierte böswillige Angriffe wie Prompt Injections und Jailbreak-Versuche automatisch abzuwehren. Guardrails sorgt darüber hinaus für eine verantwortungsvolle KI-Nutzung, da schädliche oder diskriminierende Inhalte herausgefiltert und die Bereitstellung urheberrechtlich geschützter Materialien blockiert werden. Durch die Kombination dieser DLP- und Guardrail-Funktionen können Unternehmen ihre Benutzer proaktiv coachen und gleichzeitig ihr gesamtes KI-Ökosystem vor Datenlecks und neuen Bedrohungen schützen.

Schritt 4: Private KI-Anwendungen

Wie können wir bei der Entwicklung privater KI-Anwendungen schädliche oder verzerrte Modellausgaben und häufig auftretende Anwendungsschwachstellen verhindern?

Unternehmen in stark regulierten Branchen (z. B. Gesundheitswesen, Finanzdienstleistungen, öffentliche Verwaltung) übernehmen bei der Entwicklung privater KI-Anwendungen eine Vorreiterrolle. Während ihr Vertrauen in die KI zunimmt, verwenden viele Unternehmen vor Ort betriebene Modelle und trainieren sie mit ihren eigenen Daten, um die mit der Datenhoheit, dem Datenschutz, der Compliance und den Drittanbietern verbundenen Risiken zu reduzieren und gleichzeitig die Relevanz und Zuverlässigkeit zu verbessern.

Ein Drittel aller Unternehmen nutzt bereits OpenAI-Services über Azure. 27 % setzen Amazon Bedrock ein, während 10 % Google Vertex AI[1] verwenden. Diese auf Unternehmen zugeschnittenen Plattformen stellen sichere, cloudbasierte KI-Services bereit, deren Datenschutzkontrollen strenger und Integrationsoptionen umfangreicher sind als bei ihren öffentlichen Versionen.

Bei der Entwicklung eigener KI-Systeme liegt die Verantwortung für die Sicherheit jedoch beim Unternehmen selbst. Neben dem Schutz vor KI-spezifischen Bedrohungen zur Laufzeit und dem Missbrauch durch Mitarbeiter gibt es noch eine weitere Angriffsfläche: Die Tools, die zur Entwicklung und Bereitstellung dieser Systeme verwendet werden, verfügen oft nicht über integrierte Sicherheitsmechanismen.

Beim lokalen Betrieb eines KI-Modells muss unbedingt überprüft werden, wie anfällig es für Schwachstellen ist. Wenn ein Unternehmen beispielsweise ein Open-Source-Modell anpasst, muss das Sicherheitsteam den Code sorgfältig prüfen, damit keine schädlichen Komponenten eingeführt werden können. Das könnte etwa Code sein, der Prompts erfassen oder an eine externe Quelle übermitteln kann.

Ferner muss darauf geachtet werden, dass die Trainingsdaten des Unternehmens keine unerwünschten Informationen enthalten. Die oft sehr umfangreichen Datensätze sollten von den Teams auf voreingenommene, sensible oder schädliche Inhalte überprüft werden.

Unser Ansatz

Durch die Zentralisierung der Authentifizierung, der Verwaltung des Datenverkehrs und der Inhaltsprüfung zwischen privaten Anwendungen und LLMs sorgt Netskope One AI Gateway dafür, dass die mit autonomen, agentenbasierten Systemen zusammenhängenden Datenflüsse kontrolliert und abgesichert bleiben. Des Weiteren testet Netskope One AI Red Teaming durch die Automatisierung von Angriffssimulationen in CI/CD-Pipelines proaktiv benutzerdefinierte Modelle auf ihre Belastbarkeit, um Schwachstellen wie Prompt Injections aufzudecken.

Netskope One AI Guardrails verhindert komplexe Angriffe – darunter Prompt Injections und Jailbreak-Versuche – durch die Echtzeitanalyse des gesamten Datenverkehrs. Gleichzeitig übernimmt es die Rolle eines Inhaltsmoderators, der die schädlichen oder diskriminierenden Inhalte bei menschlichen und agentenbasierten Interaktionen erkennt und kontrolliert.

Mit Netskope One DSPM erhalten Sicherheitsexperten zudem umfassende Transparenz und Kontrolle über ihre Daten, unabhängig davon, wo sich diese befinden. Dies hilft ihnen dabei, vertrauliche Daten zu identifizieren und zu klassifizieren, die etwa zum Trainieren eines KI-Modells verwendet werden könnten.

[1] *Netskope Threat Labs, Netskope Cloud and Threat Report 2026*

Schritt 5: Autonome Agenten

Wie können wir bei der Bereitstellung autonomer Agenten verhindern, dass zu weitreichende Zugriffsrechte gewährt werden?

Beim Hype um künstliche Intelligenz macht insbesondere die agentenbasierte KI derzeit von sich reden. Viele Experten sind sogar der Meinung, dass sie bei der Unternehmenstechnologie der Zukunft eine zentrale Rolle spielen wird. Das Marktforschungsunternehmen Gartner® sagt voraus, dass agentenbasierte KI bis zum Jahr 2028 mindestens 15 % der täglichen Geschäftsentscheidungen autonom treffen wird. 2024 waren es 0 %[1].

Zwar steckt diese Technologie noch in den Kinderschuhen, doch laut einer Studie der Netskope Threat Labs vom August 2025 gibt es bereits eine kritische Masse an Benutzern in unterschiedlichen Unternehmen, die entweder selbst KI-Agenten entwickeln oder die Funktionen agentenbasierter KI in SaaS-Lösungen nutzen.

GitHub Copilot wird heute zum Beispiel in 39 % aller Unternehmen verwendet, und in 5,5 % von ihnen setzen Benutzer Agenten ein, die auf der Grundlage gängiger KI-Agenten-Frameworks lokal erstellt wurden. Nach Angaben der Forscher gibt es in 66 % der Unternehmen Benutzer, die API-Aufrufe an api.openai.com senden, und in 13 % an api.anthropic.com[2].

39 % aller Unternehmen verwenden GitHub Copilot, und 5,5 % betreiben KI-Agenten, die lokal auf der Grundlage gängiger Frameworks generiert wurden.

Netskope, Cloud and Threat Report: Shadow AI and Agentic AI 2025

[1] *Pressemitteilung von Gartner: Gartner Identifies the Top 10 Strategic Technology Trends for 2025, 21. Oktober 2024*

[2] *https://www.netskope.com/resources/cloud-and-threat-reports/cloud-and-threat-report-shadow-ai-and-agentic-ai-2025*

Viele Unternehmen haben gegenwärtig noch keinen genauen Überblick über die Anzahl ihrer agentenbasierten KI-Ressourcen. Da sich dieser Bereich schnell weiterentwickelt und ständig neue Funktionen hinzukommen, wird agentenbasierte KI zu einem wachsenden Problem der Schatten-KI.

Je mehr KI-Agenten zum Einsatz kommen, und je breiter ihr Anwendungsspektrum im gesamten Unternehmen ist, desto größer werden die damit verbundenen Sicherheitsrisiken. Die Teams müssen daher genau verstehen, welche Aktionen die einzelnen Agenten ausführen, damit geeignete Kontrollmechanismen und Richtlinien zur Verwaltung der Berechtigungen und Aktivitäten eingerichtet werden können.

KI-gestützte Anwendungen basieren auf der authentifizierten Kommunikation zwischen internen Anwendungen, autonomen Agenten und privat gehosteten LLMs. Dazu verwenden sie das Model Context Protocol (MCP) und APIs. Die Protokolle sind zwar sichere Kommunikationswege, doch die nicht menschlichen Interaktionen können eine kritische Sicherheitslücke eröffnen. Mithilfe von APIs und MCP können KI-Agenten direkt mit vertraulichen Daten und Tools interagieren und dabei die üblichen, auf Menschen ausgerichteten Sicherheitsmechanismen umgehen. Die daraus resultierende Sicherheitslücke erhöht das Risiko unbeaufsichtigter autonomer Interaktionen, was zur Offenlegung von Anmeldedaten, Tool Poisoning und unbefugter Datenexfiltration führen kann.

Unser Ansatz

Netskope One AI Gateway agiert als softwaredefiniertes Gateway, das den API-Verkehr zwischen internen Anwendungen, autonomen Agenten und privat gehosteten LLMs abfängt und steuert. Um sicherzustellen, dass nur authentifizierte Agenten mit den LLMs kommunizieren können, wird für jede Anfrage ein gültiges, vom AI Gateway generiertes Token verlangt.

Der Netskope One Agentic Broker bietet ganzheitliche Transparenz und Echtzeitschutz für MCP-fähige Anwendungen, darunter KI-Code-Editoren, Chat-Schnittstellen und Entwicklertools. Durch die Entschlüsselung und Absicherung des MCP-Datenverkehrs zwischen KI-Agenten und Datenquellen schließt er die Lücke zwischen Mensch-LLM-Interaktionen und KI-Workflows auf Maschinenebene. Dadurch wird ein einheitlicher Sicherheitsstatus gewährleistet, d. h. sensible Unternehmensdaten sind geschützt, während die Geschwindigkeit und der Umfang der agentenbasierten Automatisierung umfassend genutzt werden können.

Fazit: KI-Risikomanagement ohne Kompromisse

KI ist eine epochale Herausforderung für CIOs, CISOs und ihre Teams. Sie bietet ihnen aber auch eine einzigartige Chance. Sie verbindet sie enger mit der Geschäftsstrategie und dem Unternehmenswachstum als jemals zuvor und erhöht dadurch ihren Einfluss und ihre Reichweite. KI bringt aber auch erhebliche, sich schnell entwickelnde Risiken für Daten, Einnahmen und den Ruf des Unternehmens mit sich, die jede Sicherheitsverletzung und jeden Hackerangriff zu einer noch größeren Gefahr machen.

Um dieser Herausforderung zu begegnen, benötigen IT-Führungskräfte ein klar umrissenes Framework, das die disruptiven Möglichkeiten und die Sicherheitsanforderungen der KI verständlich macht. So erhalten sie die nötigen Fakten, um mit Kollegen aus nicht technischen Abteilungen über KI zu sprechen, die potenziellen Risiken der KI effektiv zu mindern und strenge Compliance-Standards einzuhalten.

Die Herausforderung für IT- und Sicherheitsexperten besteht heute darin, die Einführung von KI lückenlos zu sichern, damit Innovationen ohne Risiken realisiert werden können, während der Geschäftsbetrieb reibungslos weiterläuft.

Netskope One ist eine einheitliche, konsolidierte Plattform, die Unternehmen die Möglichkeit bietet, die mit KI verbundenen Risiken effektiv zu managen, ohne dabei Kompromisse bei der Leistung oder der Benutzererfahrung eingehen zu müssen. Gleichzeitig reduziert sie die Komplexität und gewährleistet die Einhaltung aller geltenden Vorschriften.

Mit der Zeit werden immer mehr Unternehmen KI einführen. Von den ersten Experimenten bis zum Einsatz agentenbasierter Systeme können IT-Führungskräfte eine entscheidende Rolle spielen und geschäftliche Innovationen vorantreiben. Durch die sichere Nutzung aller Vorteile der KI können CIOs und CISOs heute geschäftliche Ergebnisse erzielen, die ihr Unternehmen auf die nächste Entwicklungsstufe heben.

Netskope One AI Security stellt eine einheitliche Lösung zur Verwaltung Ihres KI-Ökosystems und zum Schutz Ihrer Daten bereit. Diese Lösung sichert Benutzer und automatisierte Agenten nicht nur in öffentlichen SaaS-Umgebungen ab, sondern schützt auch private KI-Tools und agentenbasierte Workflows. Durch die Kombination von leistungsstarken Funktionen mit kontextbezogenen Zero-Trust-Kontrollen hilft Netskope Unternehmen dabei, nicht nur mit KI zu experimentieren, sondern deren Potenzial auch voll auszuschöpfen.

Wenn Sie erfahren möchten, was CEOs von ihren IT-Führungskräften erwarten, lesen Sie hier den Bericht „Crucial Conversations“ von Netskope.

Über Netskope

Netskope ist ein führender Anbieter von modernen Sicherheits-, Netzwerk- und Analyselösungen für das Cloud- und KI-Zeitalter. Die einzigartige Architektur der Netskope One-Plattform bietet kontextbezogene EchtzeIT-Sicherheit für Mitarbeiter, Geräte und Daten, ganz gleich, wo sie sich befinden. Sie optimiert gleichzeitig die Netzwerkleistung, ohne Kompromisse oder Einschränkungen. Tausende Kunden und Partner vertrauen der Netskope One-Plattform, ihrer patentierten Zero-Trust-Engine und ihrem leistungsstarken NewEdge-Netzwerk, wenn es darum geht, Risiken zu minimieren, konvergierte Infrastrukturen zu vereinfachen sowie vollständige Transparenz und Kontrolle über die Aktivitäten von Cloud-, KI-, SaaS-, Web- und Privatanwendungen zu gewinnen.

Sie möchten mehr erfahren?

Demo anfordern

netskope