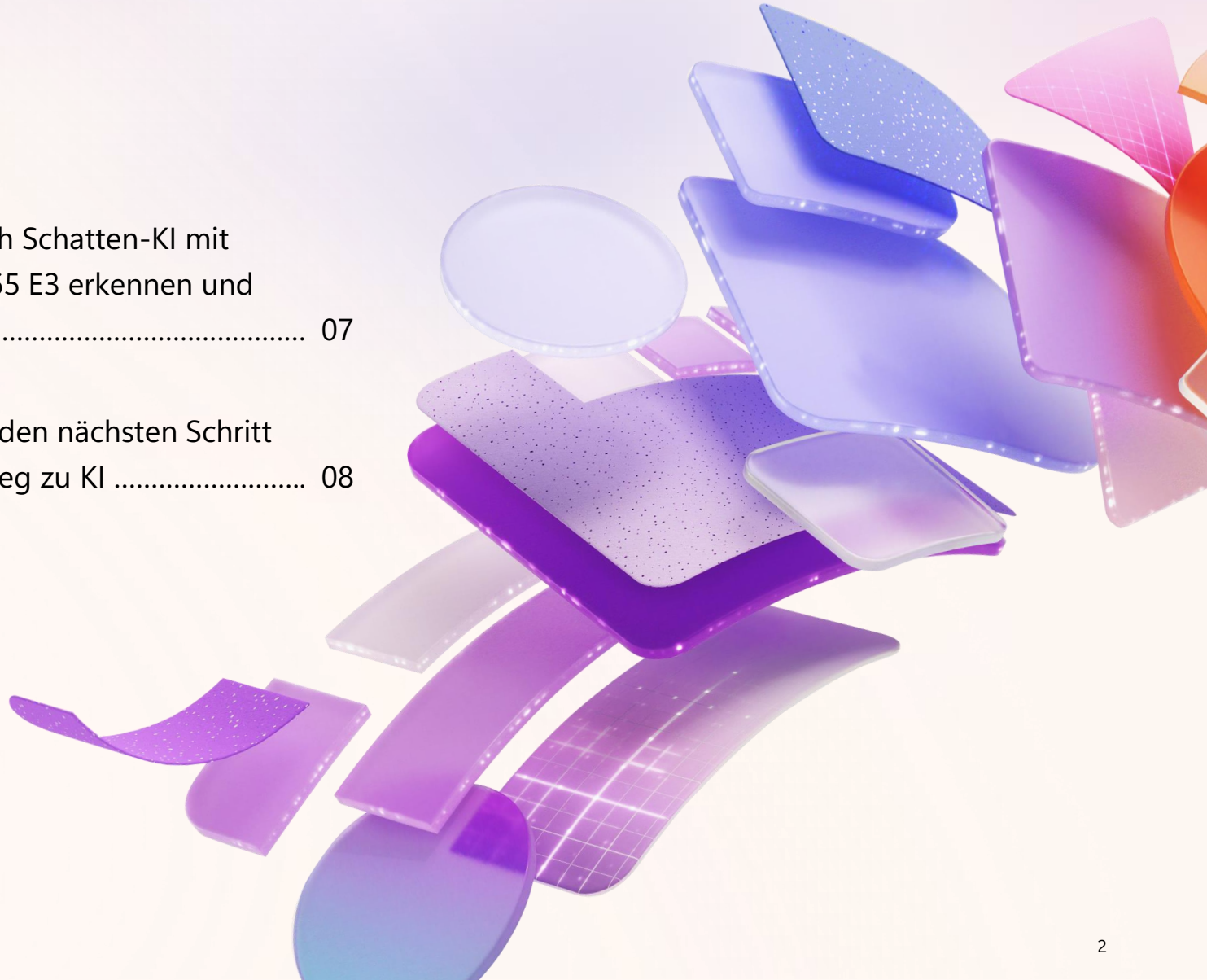
Microsoft 365

Von der Überwachung zu Insights: Verwaltung der Risiken von Schatten-KI

Inhalt



Einleitung

Im aktuellen Work Trend Index-Bericht gaben mehr als 80 % der befragten Wissensarbeitenden (Mitarbeitende und Führungskräfte) aus 31 Ländern an, dass ihnen die Zeit oder Energie fehlt, um ihre Arbeit zu erledigen. Mehr als 50 % der befragten Führungskräfte fügten hinzu, dass die Produktivität gesteigert werden müsste, um die gesetzten Ziele zu erreichen.[1] Laut Microsoft Work Trend Index Report 2024 greifen viele Mitarbeitende auf Tools zurück, die auf generativer KI (GenAI) basieren, um diese Lücke zu schließen – und warten nicht auf die offizielle Freigabe der IT, bevor sie mit deren Nutzung beginnen.

Wenn Tools außerhalb der Sichtbarkeit der IT betrieben werden, können sie für die Unternehmen Sicherheits- und Compliancerisiken mit sich bringen. Die Schatten-KI, d. h. die Nutzung von KI-Tools ohne Genehmigung der IT-Abteilung – entwickelt sich zur neuesten Form von Schatten-IT an den Arbeitsplätzen von heute.

Da die Einführung von KI immer schneller voranschreitet, arbeiten Führungskräfte daran, ihren Vorsprung zu halten und mögliche Risiken dieser Tools zu minimieren. In einer aktuellen iSMG-Studie gaben mehr als 70 % der befragten Führungskräfte an, dass sie die Sicherstellung von Datenschutz und Sicherheit als die größte Herausforderung bei der Integration von generativer KI in die bestehende IT-Infrastruktur sehen.[2] Darüber hinaus berichteten mehr als 90 % der befragten CIOs und CTOs, dass generative KI bereits zu höheren Investitionen in die Cybersicherheit in ihrem Unternehmen geführt hat oder noch führen wird.[3]

In diesem E-Book werden häufige Szenarien beschrieben, in denen Schatten-KI zum Einsatz kommt. Außerdem lernen Sie die potenziellen Risiken für Unternehmen kennen, einschließlich fünf Möglichkeiten, wie Sie diese Risiken bewältigen können, und Sie erfahren, wie Microsoft 365 E3 Ihnen dabei helfen kann.

[1] **2025 Work Trend Index Annual Report,** Microsoft, Inc., April 2025. Microsoft analysierte Umfragedaten von 31.000 in Vollzeit angestellten oder selbstständigen Wissensarbeitenden aus 31 Ländern, die zwischen dem 6. Februar und 24. März 2025 erhoben wurden, sowie LinkedIn-Arbeitsmarkttrends und Billionen von Microsoft 365-Produktivitätssignalen.

[2] **iSMG Second Annual Generative AI Study: Business Rewards vs. Security Risks,** basierend auf den Antworten von mehr als 360 Geschäfts- und Cybersicherheitsfachkräften im 3. Quartal aus sechs Regionen (Nordamerika, Europa, Asien, Südamerika, Australien und Afrika).

[3] **The AI Security Balancing Act: From Risk to Innovation", NTT DATA, Juni 2025,** basierend auf den Ergebnissen einer NTT DATA-Umfrage unter mehr als 2.300 GenAI-Verantwortlichen, darunter 1.500 Führungskräfte der C-Ebene in 34 Ländern.

Was ist Schatten-KI? Und warum ist Sichtbarkeit wichtig?

Schatten-KI bezieht sich auf den Einsatz von KI-basierten Tools und Anwendungen durch Mitarbeitende ohne ausdrückliche Freigabe oder Kontrolle durch die IT-Abteilung, häufig außerhalb der Sichtbarkeit offizieller Sicherheits- und Compliance-Frameworks. Da Mitarbeitende nach Möglichkeiten suchen, ihre Produktivität zu steigern und den wachsenden Anforderungen ihrer Arbeitslast gerecht zu werden, greifen sie möglicherweise auf nicht autorisierte KI-Lösungen zurück, um Aufgaben zu vereinfachen, zusammenzuarbeiten oder neue Inhalte zu erstellen – oft ohne sich der damit verbundenen potenziellen Risiken bewusst zu sein. Schatten-KI ist für die IT nicht sichtbar, was es für die Unternehmen schwierig macht zu wissen, welche Anwendungen genutzt werden und welche die größten Risiken bergen.

Warum Sichtbarkeit von Schatten-KI wichtig ist

Wenn das IT-Team eine Anwendung oder einen Dienst nicht kennt, kann es diese weder schützen noch Support dafür leisten. Diese *Sichtbarkeitslücke* macht es schwierig, potenzielle Bedrohungen im Zusammenhang mit der Offenlegung sensibler Daten, der Nichteinhaltung von Vorschriften und dem Kontrollverlust über proprietäre Informationen genau zu identifizieren, zu verwalten oder zu mindern. IT- und Geschäftsleitung müssen Einblick in die im Unternehmen genutzte Schatten-KI gewinnen, die mit der KI-Nutzung verbundenen neuen Risiken angehen und entscheiden, welche Tools mit geeigneten Schutzmaßnahmen zugelassen werden sollten. Für Unternehmen bietet sich die Chance, Schatten-KI von einem Risiko in eine Möglichkeit zu verwandeln, neu zu definieren, was Arbeit sicher macht.
Dazu muss ein besseres Gleichgewicht hergestellt werden, damit Mitarbeitende nützliche KI-Tools innerhalb eines geregelten, sicheren Rahmens nutzen können, um potenzielle Risiken zu minimieren.

INSIGHT

Es kann nur das geschützt werden, was man sieht. Wenn die IT-Abteilung keine Kenntnis davon hat, dass eine Anwendung oder ein Dienst genutzt wird, kann sie deren Sicherheit nicht gewährleisten. Dies ist der Kern des Problems der Schatten-KI – und zeigt, warum ein neuer Ansatz erforderlich ist. Es ist wenig sinnvoll, einfach alle externen Tools zu verbieten, wenn Mitarbeitende diese KI-Tools für das Erreichen ihrer Ziele als unerlässlich ansehen. Vielmehr müssen die Unternehmen Schatten-KI sichtbar machen – um Einblicke darin zu erhalten, welche Tools von Mitarbeitenden genutzt werden, um geeignete Kontrollen einzuführen und um sichere, freigegebene Alternativen anzubieten, die den Anforderungen des Unternehmens entsprechen. Die Herausforderung besteht also darin, Teams mit KI zu unterstützen, *ohne* die Sicherheit zu beeinträchtigen.

Schatten-KI am Arbeitsplatz: Beispielszenarien und potenzielle Risiken

Schatten-KI entsteht durch Mitarbeitende, die ihre Produktivität und Effektivität steigern oder eine neue Technologie ausprobieren möchten. Nachfolgend finden Sie einige fiktive Beispiele, die zeigen, wie nicht autorisierte KI-Tools eingesetzt werden und welche potenziellen Risiken sie bergen können:

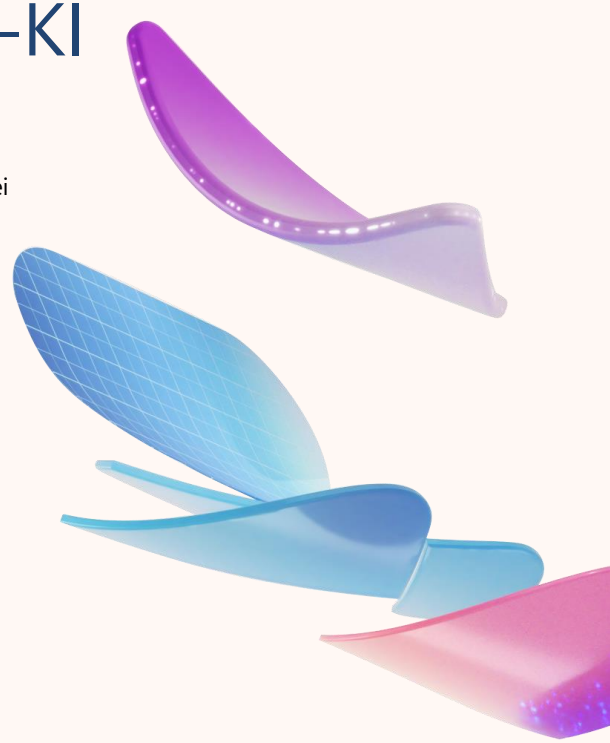
Rolle	Beispielszenario	Potenzielle Risiken durch den Einsatz nicht genehmigter Tools
Marketing	Verwendung eines GenAI-Tools zur Erstellung von Marketingtexten oder -entwürfen basierend auf Markendaten des Unternehmens	Abfluss sensibler Marken- oder Produktinformationen sowie Kontrollverlust darüber, wie ein externer KI-Dienst die kreativen Ressourcen des Unternehmens speichern oder verwenden könnte
Finanzen	Upload von Unternehmensfinanzdaten in einen KI-gestützte Analytics- oder Visualisierungsdienst, um schnelle Insights zu erhalten	Offenlegung vertraulicher Finanzdaten (Budgets, Prognosen) gegenüber Dritten; potenzielle Complianceverstöße (z. B. DSGVO), wenn Kunden- oder Mitarbeiterdaten ohne angemessene Sicherheitsvorkehrungen enthalten sind
Kundensupport	Weitergabe von Kundendaten oder Supportchatprotokollen an ein KI-Tool, um Antworten zu generieren oder Fälle zusammenzufassen	Verletzung der Datenschutz- und Datenverarbeitungsregeln – sensible Kundeninformationen könnten außerhalb der Unternehmenssysteme gespeichert werden; keine Garantien für die Datenaufbewahrung oder ordnungsgemäße Löschung der Daten durch den KI-Anbieter.
Einzelhandel	Einsatz von KI-Planungsapps durch die Filialleitung auf ihrem Smartphone, um die Schichtpläne der Mitarbeitenden zu optimieren	Mitarbeiterdaten (Namen, Schichtpläne) werden in eine nicht genehmigte App hochgeladen, wodurch Datenschutzprobleme entstehen können. Widersprüchliche Zeitpläne oder Richtlinienverstöße können auftreten, wenn KI-Vorschläge nicht mit den arbeitsrechtlichen Vorschriften übereinstimmen.
Gesundheitswesen	Nutzung eines KI-Chatbots durch medizinisches Fachpersonal, um Patientendokumentation zu verfassen oder medizinische Fragen zu beantworten	Patientengesundheitsdaten könnten ohne jegliche Sicherheitsvorkehrungen an einen externen Dienst weitergegeben werden, was gegen Compliance- und Vertraulichkeitsanforderungen verstößt. Darüber hinaus sind ggf. die medizinischen Empfehlungen nicht verifiziert; dies könnte ein Sicherheitsrisiko darstellen.

In jedem der oben genannten Fälle hatte die jeweilige Person gute Absichten und wollte produktiver arbeiten, dem Unternehmen können dadurch aber Risiken entstehen.

Unternehmensdaten könnten über nicht genehmigte Plattformen verbreitet werden, was zu *Problemen bei der Data Governance* führt. Nicht überprüfte Apps könnten Schadsoftware oder Sicherheitslücken einschleusen und die Angriffsfläche außerhalb des Aufsichtsbereichs der IT vergrößern. Es kann auch Auswirkungen auf die Compliance geben. Aus Sicht des IT-Supports kann der Helpdesk Endbenutzer möglicherweise nicht unterstützen, wenn bei einem Schatten-KI-Tool ein Fehler auftritt, da er keinen Einblick oder keine Kontrolle darüber hat.

Fünf Strategien zur Verwaltung der Risiken von Schatten-KI

Mit der richtigen Strategie und geeigneten Tools können Sie Schatten-KI von einer potenziellen Bedrohung in eine Chance verwandeln, um eine Kultur sicherer Innovationen zu fördern. Stellen Sie Ihren Teams KI-Produktivitätstools zur Verfügung *und* behalten Sie dabei die notwendige Kontrolle, um Ihr Unternehmen zu schützen. Es geht darum, ein Tool nicht unbedingt von Grund auf abzulehnen, sondern seine Verwendung mit den richtigen Schutzmaßnahmen zuzulassen. Die folgenden fünf Tipps sollen Ihnen dabei helfen, die Schatten-KI in Ihrem Unternehmen zu verwalten und zu kontrollieren:



01 Nutzung von Schatten-KI im Unternehmen erkennen, um die Risiken zu bewerten und zu priorisieren

Es kann nur das geschützt werden, was man sieht. Verschaffen Sie sich mithilfe von Aktivitätsprotokollen einen Überblick über die in Ihrem Unternehmen genutzten Anwendungen. Sobald Sie wissen, welche Apps verwendet werden, können Sie die richtigen Tools für den Umgang mit sensiblen Daten identifizieren und gleichzeitig diejenigen feststellen, die nicht mit Ihren Sicherheits- und Compliancerichtlinien übereinstimmen. Anhand dieser Insights können Sie fundierte Entscheidungen dahingehend treffen, welche Anwendungen Sie zulassen, überwachen oder einschränken möchten, um potenzielle Risiken zu minimieren.

02 Schnelle Erfolge mit Sicherheits- und Compliancerichtlinien erzielen

Ermöglichen oder implementieren Sie Richtlinienkorrekturen, um potenzielle Risiken durch den Einsatz von Schatten-KI besser eindämmen zu können. Sie können Richtlinien für den bedingten Zugriff verwenden, um die Nutzung von Anwendungen mit hohem Risiko einzuschränken. Sie können Richtlinien für die Verhinderung von Datenverlust (Data Loss Prevention, DLP) für sensible Informationen nutzen, um eine zu starke Weitergabe und Datenlecks zu verhindern, und grundlegende Multi-Faktor-Authentifizierung sowie Gerätekonformität für alle Benutzer durchsetzen. Durch diese Maßnahmen lassen sich schnell die offensichtlichsten Risiken verringern, auch wenn Sie noch keinen vollständigen Überblick über die genutzten KI-Anwendungen haben.

03 Mitarbeitende über die potenziellen Risiken von Schatten-KI aufklären

Oft sind sich Mitarbeitende der Risiken, die die Nutzung nicht genehmigter KI-Tools für ein Unternehmen darstellen kann, nicht bewusst. Informieren Sie regelmäßig über die Risiken von Schatten-KI mit gut platzierten Warnungen zur Verhinderung von Datenverlust, mit Erinnerungen an die Unternehmensrichtlinien sowie mit kurzen Trainings, um die Benutzer zu sichereren Praktiken zu bewegen – ohne allzu strikte Maßnahmen durchzusetzen.

04 Genehmigte KI-Tools bereitstellen, um die Risiken weiter zu minimieren

Bieten Sie den Mitarbeitenden nach Möglichkeit zugelassene KI-Tools als Alternative zu nicht genehmigten Tools an. Eine effektive Methode, Schatten-KI zu reduzieren, besteht darin, die häufigsten Anwendungsfälle in Ihrem Unternehmen mit einer genehmigten Lösung abzudecken. Dadurch kann die IT-Abteilung die Sichtbarkeit und Kontrolle behalten und bei auftretenden Problemen Benutzersupport bieten.

05 Fortlaufende Governance einrichten

Integrieren Sie Prüfmechanismen in Ihre IT-Governance-Routine: Überprüfen Sie regelmäßig Aktivitätsprotokolle und Berichte, aktualisieren Sie Richtlinien, sobald neue KI-Dienste herauskommen, und halten Sie die Führungskräfte über Fortschritte auf dem Laufenden (wie z. B. reduzierte Nutzung nicht genehmigter Apps oder verhinderte Vorfälle). Dadurch können Sie potenzielle Risiken jetzt und in Zukunft mindern, während sich die Landschaft weiterentwickelt.

Mit den oben genannten Schritten können Sie sowohl Innovationen als auch Sicherheit fördern.

Mitarbeitende können zugelassene KI-Lösungen am Arbeitsplatz nutzen, und die IT behält die Kontrolle und Compliance über diese Tools.

Risiken durch Schatten-KI mit Microsoft 365 E3 erkennen und verwalten

Microsoft 365 E3 bietet Unternehmen die nötigen Funktionen, um Schatten-IT zu erkennen, potenzielle Risiken zu bewerten und Sicherheits- sowie Compliancerichtlinien umzusetzen, *ohne* dass dies die Innovationsfähigkeit beeinträchtigt. Diese Suite integrierter Produktivitäts-, Sicherheits- und Verwaltungsfunktionen ermöglicht es Ihnen, Herausforderungen im Zusammenhang mit der Schatten-KI unmittelbar anzugehen.

Microsoft 365 E3-Lösung	Wie Ihnen die Lösung dabei hilft, potenzielle Schatten-KI-Risiken zu bewältigen
Cloud App Discovery	**Erkennen Sie nicht genehmigte Anwendungen, und ergreifen Sie entsprechende Maßnahmen.** Cloud App Discovery ermöglicht es Ihnen, Aktivitätsprotokolle hochzuladen und Momentaufnahmeberichte zu erstellen, um Einblick in mehr als 31.000 Cloud-Anwendungen zu erhalten – darunter über 400 GenAI-Apps. Mit dieser Lösung können Sie sehen, was in Ihrem Unternehmen von wem und wie oft verwendet wird. Und diese Informationen ermöglichen es Ihnen, fundierte Entscheidungen darüber zu treffen, welche Apps Sie zulassen möchten oder für welche Apps Sie die Nutzung einschränken möchten.
Microsoft Purview Data Loss Prevention (DLP)	**Verhindern Sie den Abfluss sensibler Daten.** Mit Microsoft Purview DLP können Sie Richtlinien definieren und anwenden, die vertrauliche Informationen erkennen und die Freigabe von E-Mails und Dateien in Microsoft 365-Diensten blockieren oder einschränken. Sie können beispielsweise eine Regel festlegen, um die Weitergabe sensibler Informationen per E-Mail oder Dateifreigabe zu überwachen, zu protokollieren oder zu unterbinden und die Benutzer zu warnen.
Microsoft Entra ID P1	**Verwalten Sie den Zugriff auf Cloud-Apps.** Microsoft Entra ID P1 bietet Richtlinien für bedingten Zugriff, um zu steuern, wer unter welchen Bedingungen auf welche Anwendungen zugreifen kann. Sie können z. B. eine Multi-Faktor-Authentifizierung verlangen oder gegebenenfalls die Anmeldung mit Unternehmensanmeldedaten auf Anwendungen beschränken, die Sie als risikoreicher eingestuft haben. Microsoft Entra ID P1 gewährt den richtigen Personen auf konformen Geräten unter genehmigten Bedingungen Zugriff auf Cloud-Ressourcen – und beschränkt den Zugriff auf nicht genehmigte Apps.
Microsoft Intune P1	**Setzen Sie Geräte- und App-Nutzungsrichtlinien durch.** Microsoft Intune P1 bietet Ihnen die Möglichkeit, verwaltete und konforme Geräte für die Arbeit zuzulassen, und stellt Ihnen Tools zur Verwaltung dieser Geräte zur Verfügung. So kann Microsoft Intune P1 beispielsweise die Installation nicht genehmigter Software auf Unternehmens-PCs verbieten oder Konfigurationen pushen, die den Zugriff auf bestimmte Websites oder Dienste einschränken.
Microsoft Defender for Endpoint P1	**Beschränken Sie den Datenverkehr zu nicht genehmigten URLs.** Microsoft Defender for Endpoint P1 hilft Ihnen dabei, Risiken durch Websites, die Sie als riskant einstufen, zu reduzieren, indem der Datenverkehr zu einer nicht genehmigten URL von verwalteten Geräten blockiert wird. Beispielsweise würden Mitarbeitende, die versuchen, auf einem Firmenlaptop eine als riskant eingestufte KI-Website zu besuchen, am Zugriff gehindert werden.

Machen Sie den nächsten Schritt auf Ihrem Weg zu KI →

Alles beginnt mit ausreichend Sensibilisierung, den richtigen Tools und einem proaktiven Plan. Microsoft 365 E3 stellt die Tools bereit, die Ihr Unternehmen benötigt, um eine stabile Sicherheitsbasis und ein Governance-Framework für KI-Lösungen einzurichten. Sie erhalten Einblick in nicht genehmigte Tools, können Richtlinien zum Schutz sensibler Daten umsetzen und die Kontrolle über Benutzerzugriff und Gerätesicherheit behalten. Gehen Sie von einer reaktiven Haltung (Schatten-KI erst finden und blockieren, nachdem sie aufgetaucht ist) zu einer proaktiven Vorgehensweise über, bei der die KI-Nutzung in sichere, verwaltete Kanäle gelenkt wird. Führen Sie die Sicherheitsbewertung für KI durch, und erfahren Sie, wie Sie Ihren Sicherheitsstatus im Hinblick auf KI verbessern können. Erfahren Sie mehr über die in Microsoft 365 for Enterprise enthaltenen Funktionen.