



Sophos AI Defense

See AI, Control AI, Secure AI

Christopher Erdmann

Senior Sales Engineer

Wie KI die Welt verändert hat

Zeit bis 100 Millionen Nutzer

ChatGPT

2
Monate

Internet

7
Jahre

Mobiltelefon

16
Jahre

Telefon

75
Jahre

KI hat alles verändert

GESCHWINDIGKEIT

Angriffe werden mit Maschinengeschwindigkeit ausgeführt, nicht mit menschlicher Geschwindigkeit.

SKALIERUNG

KI ermöglicht einen exponentiellen Anstieg des Angriffsvolumens.

UMFANG

KI erweitert die Angriffsfläche und die Komplexität der Ausführung.

KI-Tools bieten Angreifern neue Angriffsziele.



ShadowLeak

Diebstahl von E-Mail-Daten



Agentforce

ForcedLeak

Offenlegung von CRM-Daten



Copilot

EchoLeak

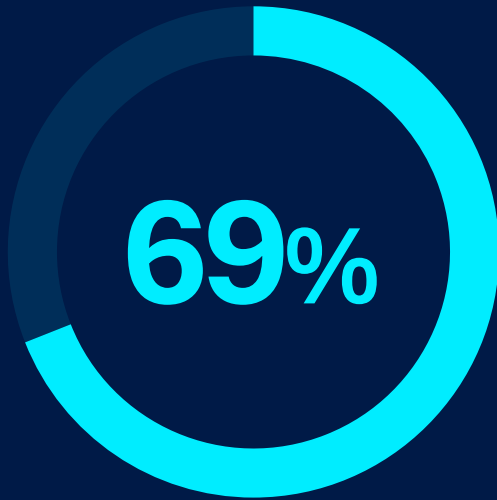
Exfiltration von Unternehmensdaten



EchoLeak

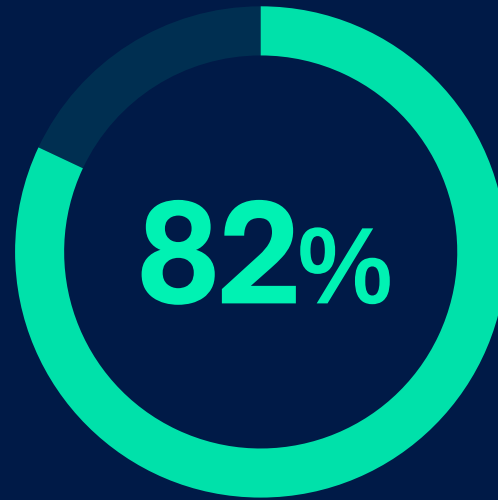


Die KI-Einführung überholt Sichtbarkeit und Kontrolle



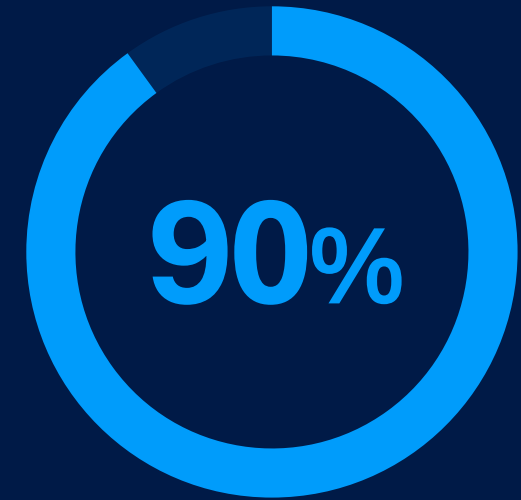
**der Organisationen haben
Belege dafür, dass
Mitarbeiter verbotene KI bei
der Arbeit nutzen**

Gartner, Gartner Cybersecurity Innovations in AI Risk Management and Use Survey.



**der Organisationen haben
unbekannte KI-Tools oder -
Workflows entdeckt**

CSA, The Shadow AI Agent Problem in Enterprise Environments 2025



**der IT-Führungskräfte sind
besorgt über das Risiko von
Schatten-KI**

Komprise IT Survey: AI, Data & Enterprise Risk



Die KI-Sicherheitslücke schließen

Was KI-Sicherheit erfordert:

- **KI erkennen:** Transparenz darüber, wie KI genutzt wird.
- **KI kontrollieren:** Durchsetzung an dem Punkt, an dem KI mit Daten in Berührung kommt.
- **KI absichern:** KI-Vorfälle werden als vollwertige Sicherheitsereignisse behandelt.

Diese Lücke schließt **SOPHOS AI Defense**.

Wir stellen vor: Sophos AI Defense

KI erkennen. KI steuern. KI absichern.

Einführung von Sophos AI Defense

Vereinheitlichen Sie Sichtbarkeit, Durchsetzung und Schutz über jedes KI-Tool, jeden Agenten und jeden Workflow.



SICHTBARKEIT

Sehen Sie jedes KI-Tool in der gesamten Umgebung

Shadow-AI-Erkennung
KI-Nutzungs-Dashboard
Endpoint + Netzwerk + Browser
mehrschichtige Erkennung



KONTROLLE

Setzen Sie KI-Richtlinien durch, ohne Innovation zu bremsen

Granulare Zugriffsverwaltung
Globale Richtliniendurchsetzung
Rollenbasierte Kontrollen
Prompt-Überwachung



SCHUTZ

Schützen Sie Daten und blockieren Sie riskantes KI-Verhalten

Eingabe bereinigen
Ausgabe abfangen
DLP für KI-Prompts

Ihre KI-Landschaft, an einem Ort

Verschaffen Sie sich einen ganzheitlichen Überblick über die KI-Nutzung in Ihrer gesamten Umgebung

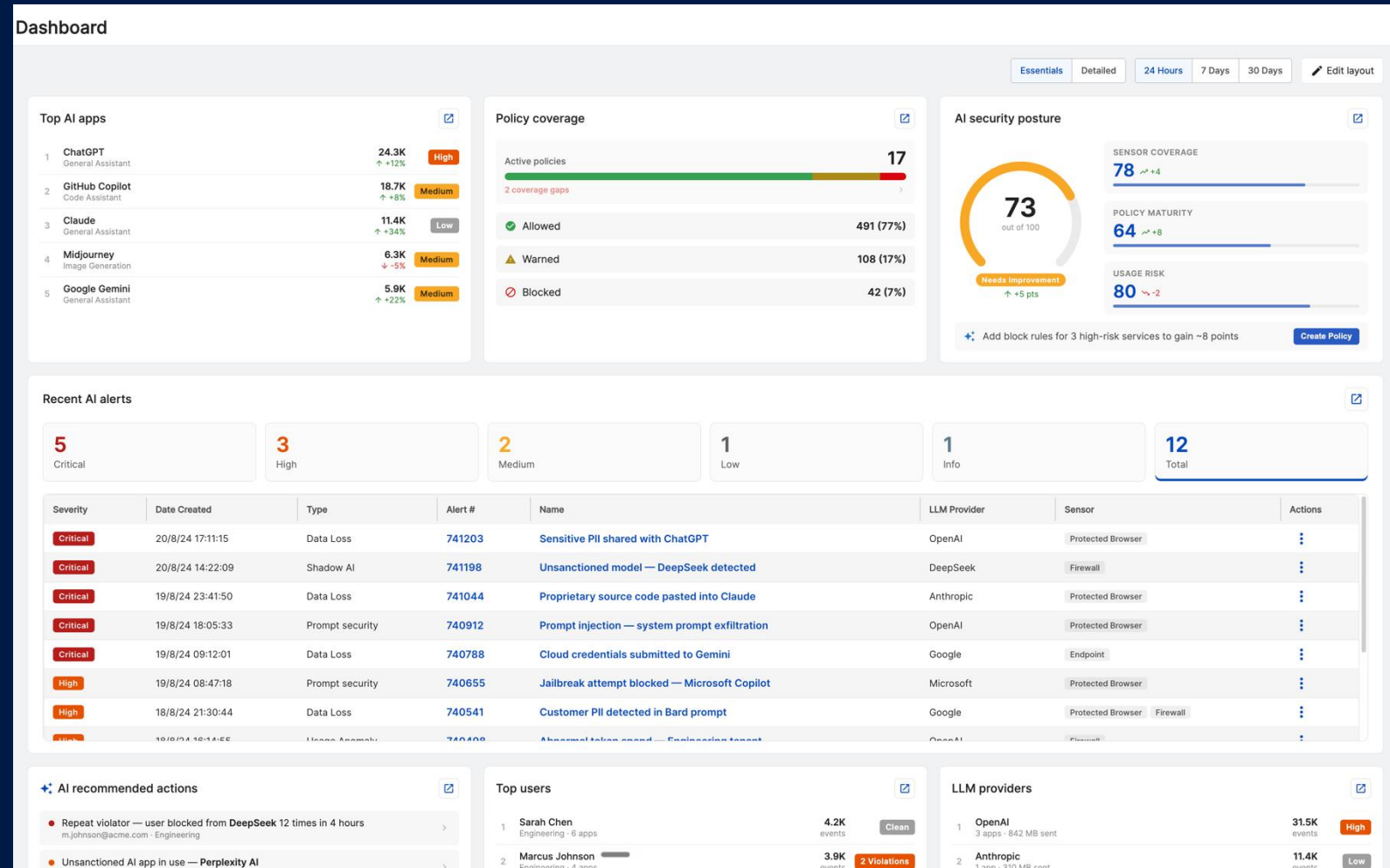
- Nicht nur, welche KI genutzt wird, sondern welche Mitarbeiter und Gruppen sie am meisten nutzen.

Verwalten Sie alle KI-Tools, Apps und Benutzer

- Granulare Kontrollen, um die Nutzung bestimmter Tools durch bestimmte Benutzer und Gruppen zu genehmigen.

Machen Sie KI-Risiken sichtbar und setzen Sie Richtlinien durch

- Kontinuierliche Überwachung, um Schutzmaßnahmen aufrechtzuerhalten und riskante Aktivitäten in Erkennungs- und Untersuchungsworkflows zu leiten.



Eine Architektur, vier Kontrollebenen

Wie sich Sophos AI Defense in das Sophos-System integriert.

01

Gerät und Identität

Sophos EDR

Benutzer- und geräteabhängige KI-Zugriffskontrollen, die mit dem Identitätskontext verknüpft sind.

02

Netzwerk

Sophos Firewall

KI-Dienstverkehr wird auf verwalteten und nicht verwalteten Geräten kontrolliert.

03

Operative Reaktion

Sophos XDR und Sophos MDR

KI-Aktivitäten werden in bewährten SecOps-Workflows verarbeitet.

04

Benutzerinteraktion

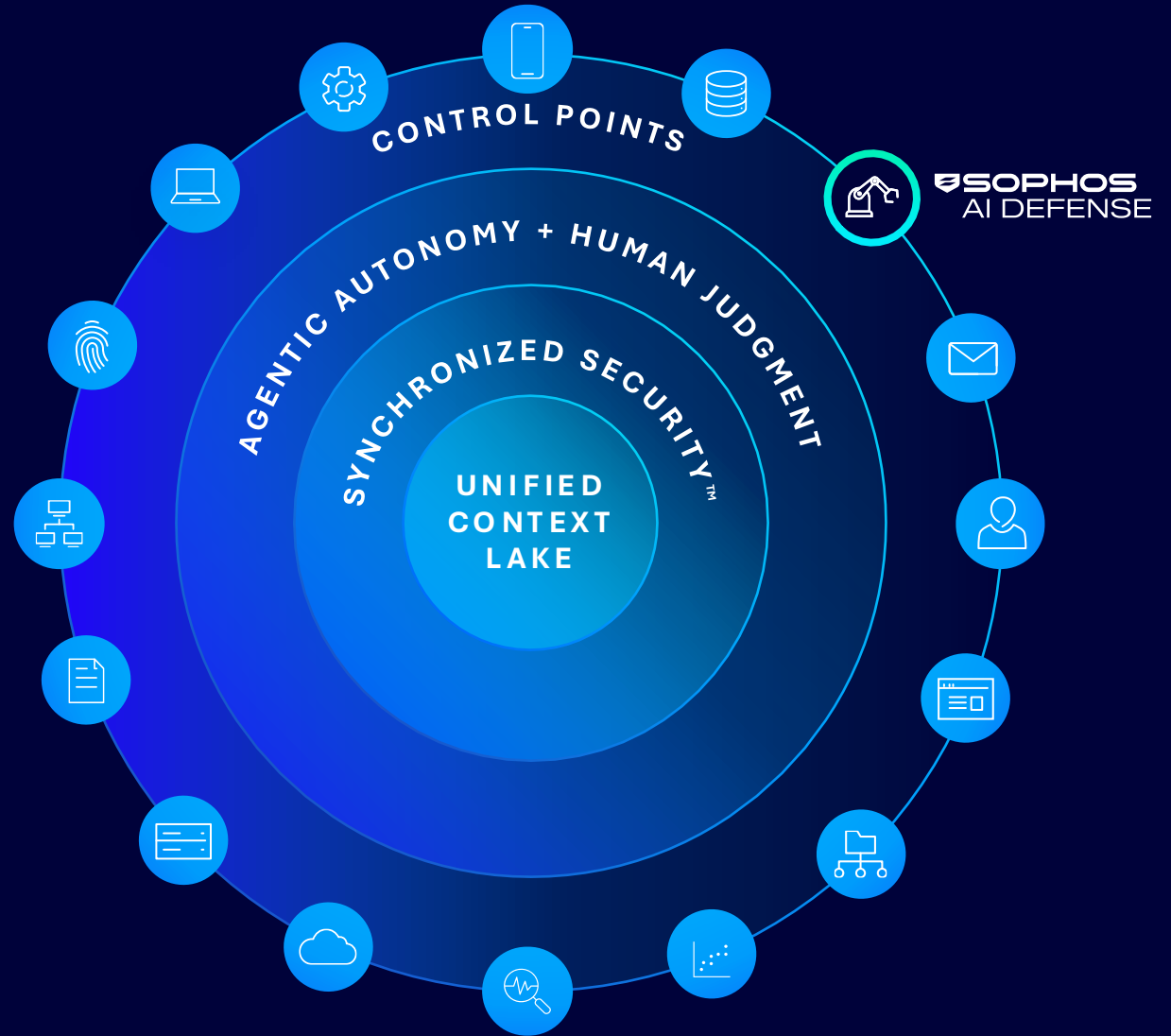
Sophos Workspace Protection

Sichtbarkeit und Kontrolle auf Browser-Ebene darüber, wie Mitarbeiter KI-Tools nutzen.

FUSION

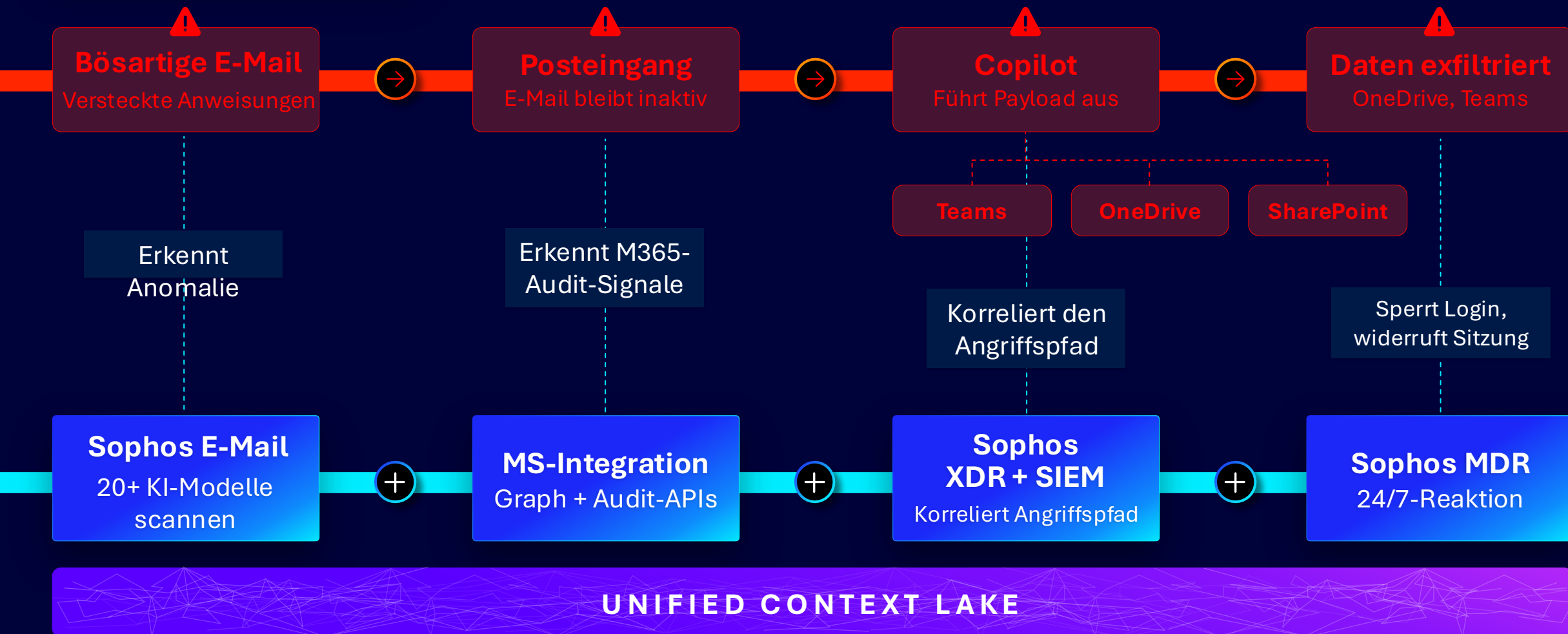
 **SOPHOS**

AI-Native
Cybersecurity
Defense System





EchoLeak



KI-Fragen? Sophos AI Defense liefert die Antworten

Fragen, die wir jeden Tag hören	Sophos AI Defense bietet
Welche KI wird in meinem Unternehmen genutzt, von wem und wo?	Transparenz über die KI-Nutzung nach Typ, Mitarbeiter und Gruppe
Ich habe KI-Tools für den Einsatz genehmigt. Nutzen meine Mitarbeiter sie?	Bestätigung, dass genehmigte Tools genutzt werden, mit Identifizierung der Nutzung nicht genehmigter Tools.
Nutzen meine Anwender KI verantwortungsvoll?	Kontextbezogene Bewertung, die akzeptable Nutzung von riskanten, überprivilegierten oder nicht zugeordneten Aktivitäten unterscheidet.
Wie kann ich der Führungsebene und dem Vorstand schnell mitteilen, wie wir KI-Risiken angehen?	Vorstandsreife Berichterstattung mit einem einzigen KI-Posture-Score.
Wie kann ich KI proaktiv verwalten, bevor die nächste virale App erscheint?	Kontinuierliche Erkennung aufkommender und Schatten-KI, sodass neue Tools kontrolliert werden, sobald sie auftauchen.
Welche Richtlinien empfehlen Sie mir, um meine sensiblen Daten zu schützen?	Empfohlene Standardrichtlinien plus Echtzeitprüfung von Prompts und Uploads, um sensible Daten aus KI-Tools herauszuhalten.
Welche KI-Tools oder -Anbieter sollte ich nicht flächendeckend einsetzen?	Risikobasierte Einstufung von Tools und Anbietern unter Berücksichtigung von Datenexposition und Modellgeografie.
Welche Agenten sind in meiner Umgebung aktiv und auf welche Daten können sie zugreifen?	Ein Inventar aktiver Agenten, einschließlich autonomer, mit Berechtigungen und Datenzugriff.
Nutzen meine Mitarbeiter KI für nicht arbeitsbezogene Zwecke?	Nutzungstransparenz auf Anwender- und Kontoebene zur Identifizierung privater Nutzung.
Wie reagiere ich, wenn mein Cyberversicherer fragt, wie wir KI verwalten?	Audit-fähige Berichterstattung über die Richtlinieneinhaltung, die dokumentiert, wie KI verwaltet und kontrolliert wird.



Securing the AI Era

AI-Native Cybersecurity Defense System