

Proofpoint AI Security

Einheitliche Transparenz, Richtliniendurchsetzung zur Laufzeit und rechtssichere Audit-Protokolle für KI-gestützte Anwendungen, KI-Agenten und MCP-Server

Wichtige Vorteile

- **Transparenz zu allen Arten von Unternehmens-KI**, einschließlich Mitarbeitertools, in Anwendungen eingebetteter KI, autonomer Agenten und MCP-Server
- **Richtliniendurchsetzung zur Laufzeit**, die Aktionen basierend auf der jeweiligen Interaktion zulässt, blockiert, ändert, einschränkt oder eskaliert
- **Rechtssichere Audit-Protokolle** für alle Verantwortlichen zur vollständigen Rekonstruktion von Transaktionen, einschließlich Anwenderanfrage, Agentenaktionen und Ergebnis
- **SOC-taugliche KI-Telemetrie** mit nativer SIEM- und SOAR-Integration, die zwischen Sicherheitsvorfällen und Governance-Verstößen unterscheidet

Das Problem

Viele Unternehmen haben keinen Überblick darüber, welche KI in ihren Umgebungen vorhanden ist, wer sie verwendet und welche Daten gefährdet sind oder sogar schon kompromittiert wurden. Diese grundlegenden Herausforderungen bei der sicheren KI-Nutzung verstärken sich mit zunehmender Reife der Technologie immer weiter.

KI-Tools sind nicht mehr nur über Webbrowser verfügbar, sondern inzwischen in viele SaaS-Anwendungen (Software-as-a-Service) eingebettet. Sie führen in zunehmendem Maße autonome Workflows aus, die sich über mehrere Unternehmenssysteme erstrecken. Zudem stellen sie über MCP-Server (Model Context Protocol) Verbindungen zu Unternehmensressourcen her. Vielen Sicherheitsteams fehlt der Überblick darüber, welche KI-Tools die Mitarbeiter verwenden und auf welche Ressourcen diese Tools zugreifen können.

Herkömmliche Sicherheitsprodukte können nicht erkennen, wenn ein Agent Aktionen ausführt, die über den Umfang der ihm übertragenen Aufgabe hinausgehen. Bei dieser Bedrohung, die als semantische Rechteerweiterung bezeichnet wird, sind die einzelnen Berechtigungsprüfungen erfolgreich, die Aktionen des Agenten führen aber dennoch zu einem Sicherheitsvorfall.

Die Berechtigungen mögen gültig sein, doch die Absicht ist manipuliert. Und die sich ändernde Absicht kann durch Verhaltensänderungen erkannt werden. Für den Schutz von KI muss bewertet werden, ob die Zugriffe, die Absicht und das Verhalten zusammenpassen.

Der Proofpoint-Ansatz: KI-Integrität

Die meisten Anbieter für KI-gerechte Sicherheitslösungen konzentrieren sich nur auf eine Dimension: Absichtserkennung, Zugriffskontrolle oder Verhaltensüberwachung. Diese Ansätze bringen jedoch die folgenden Probleme mit sich:

- Durch Zugriffskontrolle erfahren Sie, worauf ein Agent zugreifen kann, aber nicht, ob er es für eine bestimmte Aufgabe tun sollte.
- Durch Absichtserkennung erfahren Sie, was ein Anwender oder Agent vorhatte, aber nicht, ob nachgelagerte Aktionen den gültigen Berechtigungsbereich einhalten.
- Durch Verhaltensüberwachung erfahren Sie, was passiert ist, aber nicht, ob die Aktion autorisiert wurde oder mit der ursprünglichen Anfrage abgestimmt ist.

Im Gegensatz dazu beobachtet, bewertet und verifiziert Proofpoint AI Security, ob Zugriffe, Absicht und Verhalten zueinander passen. Denn nur dann agiert KI mit Integrität. Wenn dies nicht der Fall ist, kann es zu Sicherheitsvorfällen kommen – auch dann, wenn die einzelnen Genehmigungsprüfungen alle bestanden werden. Dies ist der entscheidende Unterschied zwischen KI-Integrität und KI-Sicherheit.

Schutz für Ihre KI auf jeder Ebene

Absichern der Nutzung der KI durch Anwender

Proofpoint erkennt Schatten-KI in geräteinternen Anwendungen, Cloud-Diensten und MCP-Servern. Dadurch erhalten Sicherheitsteams einen Überblick darüber, welche KI-Tools die Mitarbeiter verwenden und wo vertrauliche Daten möglicherweise gefährdet werden. Proprietäre Erkennungsmodelle analysieren den Inhalt und das Verhalten jedes einzelnen Prompts und jeder Antwort.

Die Erkennungsmodelle bewerten zudem das Risiko jeder Interaktion unter Berücksichtigung von Vertraulichkeit der Daten, Sicherheitsstatus des Anbieters und Nutzungshäufigkeit. Wenn Interaktionen gegen Richtlinien verstoßen, blockieren oder kennzeichnen konfigurierbare Kontrollen zur zulässigen KI-Nutzung diese Aktionen entsprechend der jeweiligen Anwendergruppe. Durch diesen Ansatz wird die sichere Nutzung unterstützt, ohne Anwender zu Schatten-KI zu verleiten.

Absichern der Nutzung von KI durch Agenten

Proofpoint bietet Agenten vollständige Transparenz und Sicherheit zur Laufzeit, ohne dass Codeänderungen erforderlich sind. Das gilt sowohl im Transparenzmodus als auch im Inline-Durchsetzungsmodus. Die absichtsbasierte Zugriffskontrolle (IBAC) bewertet, ob die Aktionen der Agenten zur ursprünglicher Aufgabe passen. Auf diese Weise können semantische Rechteerweiterungen erkannt werden, bevor sie zu unangemessenen Aktionen führen. Die gesamte Ausführungskette wird mit sicherheitsannotierter Forensik erfasst, die jeden Schritt, jeden Tool-Aufruf und jede Dateninteraktion bis zur ursprünglichen Anfrage zurückverfolgt.

Absichern der Interaktionen von KI mit Unternehmenssystemen

Das MCP-Gateway ist ein zentraler Kontrollpunkt für den gesamten MCP-Datenverkehr. Kein großes Sprachmodell (LLM) kann ohne MCP-Gateway-Prüfung eine Verbindung zu Unternehmensdatenquellen herstellen. Eine Registrierung von über 800 sicheren MCP-Servern mit Überprüfung der Lieferkette kann jeden neuen Server von der Quelle aus in weniger als 15 Minuten absichern. Alle Verbindungen werden authentifiziert und auf vertrauliche Daten, Prompt-Injection-Versuche und Richtlinienverstöße überprüft.

Geschäftliche Vorteile

Schnellere Einführung von KI

Sicherheitsteams können die Einführung von KI mit dem Wissen unterstützen, dass die Governance in den Bereitstellungspfad integriert ist. KI-Programme werden innerhalb von Wochen statt Monaten vom Pilotprojekt zur Produktion überführt.

Geringeres Risiko

Die Angriffsfläche reduziert sich auf das, was bekannt ist und kontrolliert sowie aktiv überwacht wird. Dies gilt für jede Form von Unternehmens-KI – von Chatbots bis hin zu autonomen Agenten.

Rechtssichere Audits ohne manuelle Rekonstruktion

Jede KI-Interaktion liefert die Beweise, die ein rechtssicheres Audit erfordert. Die Fähigkeit zur Einhaltung von Compliance-Vorgaben wird zu einem kontinuierlichen Zustand statt zu einer Stressphase, die sich jedes Quartal wiederholt.

Skalierbare Sicherheitsabläufe

Die nahtlose Integration mit SIEM-Systemen (Sicherheitsinformations- und Ereignis-Management) und SOAR-Systemen (Koordination und Automatisierung von Sicherheitsmaßnahmen) bietet KI-spezifische Telemetrie mit vollem Kontext. Sicherheitsteams können KI besser abdecken, ohne ein dediziertes KI-Sicherheitsteam einstellen zu müssen.

Funktionen von Proofpoint AI Security

FUNKTION	BESCHREIBUNG	VORTEIL VON PROOFPOINT
Kontrolle der KI-Nutzung	Erkennt KI-Nutzung in SaaS, IDE-Erweiterungen, Desktop-Anwendungen, CLI-Tools, Browser-Plugins und lokalen Modellen. Führt kontextbezogene Risikobewertungen auf Basis von Vertraulichkeit der Daten, Sicherheitsstatus des Anbieters und Nutzungshäufigkeit durch.	Governance für die KI-Nutzung auf semantischer Ebene, nicht basierend auf grundlegender URL-Filterung; Risikobewertung jeder Interaktion, nicht nur Überprüfung, ob die Nutzung eines Tools zulässig ist
AI Security Posture Management	Erstellt ein umfassendes Inventar aller KI-Anwendungen, Agenten, Tools, Integrationen, externen Dienste und MCP-Server. Bewertet den Sicherheitsstatus kontinuierlich während des gesamten KI-Lebenszyklus.	Erkennung einschließlich Agenten-Tool-Ketten und MCP-Serverinventar mit Abbildung des gesamten Ausführungsdiagramms, nicht nur der Chat-Schnittstellen
KI-Schutz zur Laufzeit	Untersucht KI-Interaktionen zur Laufzeit und bewertet Prompts, Ausgaben und Modellverhalten inline. Nutzt 18 integrierte Detektoren für alle Modi.	Bewertung auf semantischer Ebene mit Unterscheidung zwischen legitimem Verhalten und ungewöhnlichen oder manipulierten Aktivitäten zur Reduzierung von False Positives, die das Vertrauen des SOC-Teams (Security Operations Center) untergraben
Schutz des KI-Agenten-Ökosystems	Vermeidet semantische Rechteerweiterung mit absichtsbasierter Zugriffskontrolle (IBAC). Erfasst die Anwenderabsicht und stellt sicher, dass sie während des gesamten Agenten-Workflow eingehalten wird.	IBAC-gestützte Überprüfung der Absicht jeder Aktion; Erkennung von Verhaltensanomalien, Agentenmanifeste für Policy-as-Code und vollständige Transaktionsforensik während der gesamten Agentenkette
Absicherung der KI-Lieferkette	Das MCP-Gateway erzwingt die Authentifizierung und Inhaltsprüfung für den gesamten Tool-Zugriff. Erkennt und registriert alle verwendeten MCP-Server.	Durchsetzung zur Laufzeit, um festzulegen, welche Daten MCP-Grenzen überschreiten dürfen und welche Aktionen über Protokollverbindungen zulässig sind

Demo anfordern

Kontaktieren Sie Ihr Proofpoint-Kundenteam, um eine Demo von Proofpoint AI Security zu vereinbaren, oder besuchen Sie proofpoint.com/de, um mehr zu erfahren.

proofpoint.

Proofpoint ist eine eingetragene Marke bzw. ein registrierter Handelsname von Proofpoint, Inc. in den USA und/oder anderen Ländern. Alle weiteren hier genannten Marken sind Eigentum ihrer jeweiligen Besitzer.