

SOFTWAREONE UND SKYHIGH SECURITY

Sicherheit und Compliance für Enterprise ChatGPT

Sichere KI-Produktivität ohne Kompromisse ermöglichen

RISIKO-/BEDROHUNGSVEKTOR

Die unüberwachte Nutzung von Enterprise ChatGPT bringt kritische Risiken für Datensicherheit und Compliance mit sich:

- **Datenexfiltration:** Unbeabsichtigter Abfluss sensibler Daten über KI-Prompts und Ausgaben.
- **Zugriff auf sensible Daten:** Beschäftigte rufen interne Dokumente oder Erkenntnisse ab, die über ihre Zugriffsrechte hinausgehen.
- **Prompt Injection und Jailbreaks:** Bössartige Prompts manipulieren das Modell, sodass eingeschränkte Informationen offengelegt werden.
- **Compliance-Verstöße:** Verstöße gegen DSGVO, HIPAA und CCPA durch unüberwachte KI-Interaktionen.
- **Shadow-AI-Nutzung:** Nicht autorisierte Nutzung von ChatGPT-Plugins von Drittanbietern oder nicht verwalteten Konten.

Das Potenzial von Enterprise ChatGPT

Enterprise ChatGPT verändert die Produktivität, indem es Recherche, Analyse, Zusammenfassung und Ideenfindung in IT-, HR-, Rechts- und Marketingteams beschleunigt. SoftwareOne und Skyhigh Security bieten eine umfassende, speziell entwickelte Lösung, um sensible Unternehmensdaten zu schützen und Organisationen zugleich dabei zu unterstützen, das Produktivitätspotenzial von Enterprise ChatGPT vollständig zu nutzen.

Funktionen von SoftwareOne und Skyhigh Security für Enterprise ChatGPT

- 01 DLP für Prompts und Antworten:** Verhindert die Exfiltration sensibler Daten in Benutzeranfragen und KI-generierten Ausgaben.
- 02 DLP für Dateien:** Schützt sensible Dateien, unabhängig davon, ob sie von Benutzenden hochgeladen oder von ChatGPT generiert wurden, vor nicht autorisierter Freigabe oder Offenlegung.
- 03 Proaktive Compliance-Durchsetzung:** Setzt regulatorische Compliance für DSGVO, HIPAA und CCPA mit erweiterten DLP-Klassifizierungen für strukturierte und unstrukturierte Daten durch.
- 04 Bedrohungsuntersuchung mit Anomalieerkennung:** Erkennt ungewöhnliche Benutzerinteraktionen und Aktivitätsmuster, die auf Insider-Bedrohungen oder kompromittierte Konten hinweisen können.
- 05 Bedrohungsuntersuchung mit KI-Interaktionsverlauf:** Protokolliert jede KI-Sitzung mit Benutzer, Zeitstempel, Prompt, Antwort und Datenklassifizierung – für forensische Transparenz bei verdächtigen Nutzungsmustern.
- 06 User and Entity Behavior Analytics (UEBA):** Überwacht kontinuierlich Anmeldetrends, Zugriffsmuster und Datennutzung, um Abweichungen vom normalen Verhalten zu erkennen.
- 07 Shadow-AI-Erkennung und -Kontrolle:** Erkennt und kontrolliert die nicht autorisierte Nutzung von ChatGPT und anderen generativen KI-Tools im gesamten Unternehmen.
- 08 Schutz für verwaltete und nicht verwaltete Geräte:** Stellt eine konsistente Sicherheitsdurchsetzung auf Unternehmens- und Privatgeräten sicher und reduziert so Risiken durch Datenabfluss.

Warum SoftwareOne und Skyhigh Security?



Speziell entwickelt für KI-Sicherheit

Bietet KI-bewusste Schutzmechanismen für neue Risiken wie Prompt-Manipulation, Shadow AI und Datenabfluss



Branchenführende DLP-Lösung

Bewährte, unternehmenstaugliche DLP mit tiefgehender Inhaltsprüfung, Kontextbewusstsein und Echtzeitdurchsetzung



Erweiterte DLP-Verfahren (EDM, IDM, OCR)

Erkennt sensible Daten in strukturierten und unstrukturierten Quellen, sogar in Bildern und Screenshots



Einheitliche Sicherheit für KI, Web und SaaS

Erweitert konsistenten Datenschutz auf Enterprise ChatGPT, Microsoft Copilot und andere Produktivitätsanwendungen mit KI

Das volle Potenzial von ChatGPT sicher erschließen

Ermöglichen Sie Ihrer Organisation KI-Agilität, ohne Daten, Compliance-Position oder Vertrauen zu gefährden. Als Advanced Partner von Skyhigh Security kombiniert SoftwareOne führende Datenschutztechnologien mit umfassender Security- und Compliance-Expertise. Gemeinsam unterstützen wir Unternehmen dabei, Sicherheitsanforderungen in produktive KI-Nutzung zu übersetzen und den Einsatz von Enterprise ChatGPT kontrolliert und skalierbar zu gestalten.



Kontaktieren Sie uns

Besuchen Sie uns auf
www.softwareone.com

DE
T. +49 341 2568 000
E. info.de@softwareone.com

AT
T. +43 1 878 10 0
E. info.at@softwareone.com

CH
T. +41 844 44 55 44
E. info.ch@softwareone.com