LÖSUNGSÜBERSICHT

Schritte, die Sie jetzt unternehmen können, um GenAI-Risiken entgegenzuwirken

Der Einsatz von generativer KI in Unternehmen nimmt rasant zu. Erfahren Sie, wie Sie die Vorteile nutzen und gleichzeitig die Risiken minimieren können.

In einem Begleitpapier, Wie GenAI den modernen Arbeitsplatz prägt, haben wir den Einsatz von generativer KI im Unternehmen auf der Grundlage unserer eigenen Metriken und der Berichte von Branchenexperten und Analysten untersucht. In diesem Papier gaben wir Einblicke in einige Trends, die wir im Zusammenhang mit dem Einsatz von GenAI beobachten, sowie in die Art und Weise, wie sich GenAI weiterentwickelt, einschließlich der zunehmenden Verwendung von Phishing und Deepfakes. Und wir erörterten, wie wichtig es ist, den Schutz vor den zunehmenden Bedrohungen zu automatisieren, die von der Nutzung von GenAI ausgehen, und zwar sowohl durch die Handlungen uninformierter Benutzer innerhalb des Unternehmens als auch durch die böswillige Nutzung durch Außenstehende.

In diesem Beitrag gehen wir auf diese letzte Erkenntnis ein und erläutern, welche Schritte Sie unternehmen können, um Ihr Unternehmen zu schützen, während Sie den Aufstieg von GenAI im Unternehmen steuern. Wir werden auch Lösungen erörtern, die Sie jetzt schon implementieren können, um die Risiken und Herausforderungen von GenAI zu mindern.

Es ist an der Zeit, eine Strategie für die sichere Nutzung von GenAI umzusetzen

Wir wissen, dass der weltweite Datenverkehr auf GenAI-Sites zunimmt. Anhand der Kennzahlen von Menlo Security wurde in einem einzigen Quartal 2025 ein Anstieg dieses Datenverkehrs um 70 Prozent festgestellt. Darüber hinaus wird erwartet, dass der Einsatz von GenAI weltweit weiter zunehmen wird, wodurch die Nutzung von KI auf einen Kollisionskurs mit regional spezifischen Vorschriften und Gesetzen geraten wird. In einigen großen Unternehmen, darunter Meta, Box, Shopify, Microsoft und Amazon, wird der Einsatz von KI sogar zunehmend gefordert, insbesondere in Fällen, in denen menschliches Denken auf höherer Ebene nicht erforderlich ist.[1]

[1] https://www.washingtonpost.com/business/2025/06/03/ai-workplace-duolingo-shopify-employees/

Schritte, die Sie jetzt unternehmen können, um GenAI-Risiken entgegenzuwirken

Neben dem rasanten Wachstum von GenAI muss sich jedes Unternehmen mit der Tatsache auseinandersetzen, dass Angreifer selbst KI einsetzen, einschließlich der Erstellung von gefälschten KI-Websites, die sich als legitime Websites ausgeben. Erinnern Sie sich daran, wie einfach es früher war, Phishing-Versuche zu erkennen? Das ist jetzt nicht mehr so. Die KI hilft den Angreifern, E-Mails und SMS-Nachrichten zu erstellen, die völlig überzeugend sind. Sie betten bösartiges JavaScript in dynamische Webseiten ein, erstellen gefälschte Inhalte und vieles mehr.

Selbst wenn Sie keine strengen Richtlinien für die Nutzung von GenAI in Ihrem Unternehmen aufgestellt haben, müssen Sie Ihr Unternehmen vor Angreifern schützen, die sich diese Technologie bereits heute zunutze machen.

Die gute Nachricht ist, dass es Leitplanken gibt, die Sie jetzt implementieren können, einschließlich des Menlo-Ansatzes zur Bewältigung der Probleme, die GenAI mit sich bringt. Es gibt zwar viele verschiedene Ansätze, um GenAI sicher zu nutzen, aber Menlo kann innerhalb weniger Tage aktiviert werden, erfordert kein kostspieliges Umrüsten und ist mit den Tools und Technologien kompatibel, die Sie wahrscheinlich bereits einsetzen, einschließlich Ihres Browsers.

Die Menlo-Lösung basiert auf unserem einzigartigen Secure Cloud Browser, der wie ein gehärteter digitaler Zwilling der lokalen Browser der Benutzer funktioniert und alle aktiven Inhalte in der Cloud ausführt. Dies war noch nie so wichtig wie heute, da dynamische Webseiten viele Elemente enthalten, die während der gesamten Browsersitzung aus verschiedenen Quellen abgerufen werden. Angreifer verwenden KI, um Elemente wie JavaScript umzuschreiben und so eine Erkennung zu vermeiden. Der Secure Cloud Browser scannt den Datenverkehr kontinuierlich und automatisch, und die patentierte Adaptive Clientless Rendering-Technologie sorgt für eine nahtlose Leistung.

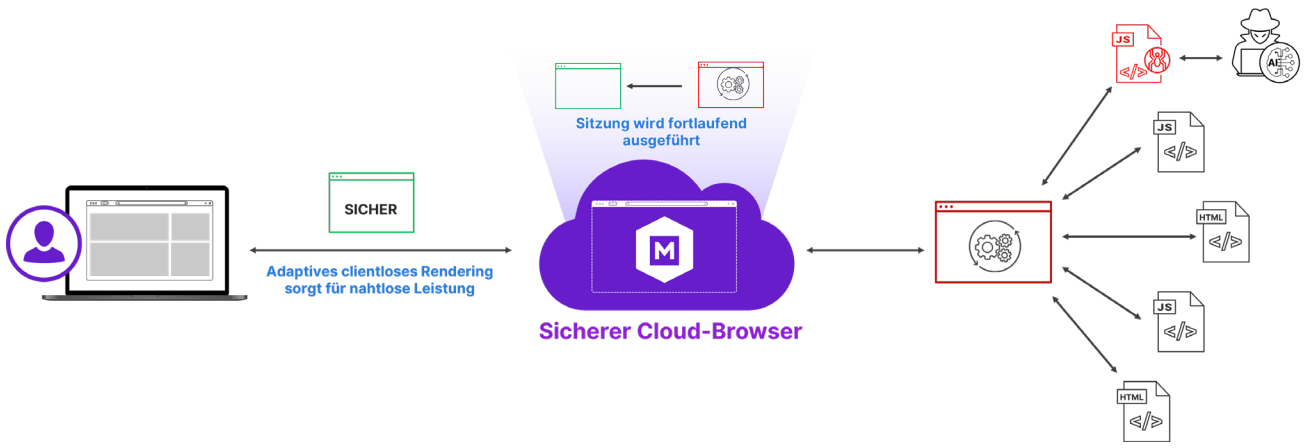

Abbildung 1: Der Menlo Secure Cloud Browser bietet während der gesamten Browsersitzung kontinuierlichen Schutz vor bösartigen Webelementen, ohne die Leistung zu beeinträchtigen oder Änderungen am Endpunkt vorzunehmen.

Beseitigen Sie „Shadow AI“

Bei der Einführung von GenAI-Tools und -Diensten waren einzelne Nutzer den Unternehmen deutlich voraus. Viele dieser Personen haben sich mit ihren eigenen Zugangsdaten für GenAI-Dienste angemeldet und sich in der Regel für die kostenlose Version entschieden. Dieses Phänomen ist als Schatten-KI bekannt und seine Nutzung wirft für die Unternehmen, in denen diese Nutzer tätig sind, heikle Fragen auf.

Erstens verliert das Unternehmen in einer solchen Situation den Überblick und die Kontrolle über wichtige Daten und Ressourcen. Zweitens verwenden die meisten kostenlosen Dienste die in Form von Abfragen übermittelten Daten, um ihre Modelle zu trainieren. Eine kürzlich durchgeführte Umfrage ergab, dass fast sieben von zehn (68 Prozent) Unternehmensmitarbeitern, die GenAI bei der Arbeit nutzen, angeben, dass sie über persönliche Konten auf öffentlich verfügbare GenAI-Assistenten wie ChatGPT, Microsoft Copilot oder Google Gemini zugreifen, und mehr als die Hälfte (57 Prozent) hat zugegeben, dass sie sensible Informationen in diese eingegeben haben.[2]

> „Das Problem ist, dass versteckte [KI]-Tools die Sicherheit gefährden, Compliance-Regeln verletzen und ungenaue oder voreingenommene Ergebnisse fördern.“ [3]
>
> – Cloud Security Alliance

Neben Problemen mit der Sichtbarkeit müssen Unternehmen auch damit kämpfen, dass Angreifer KI-Tools einsetzen, um überzeugende Angriffe und Deepfakes zu erstellen, und dass sie bekannte KI-Tool-Websites gut imitieren können. In seiner Untersuchung beobachtete Menlo bösartige Websites, deren Domainnamen „ChatGPT“, „Copilot“ oder „Gemini“ enthielten – und diese gefälschten Websites verwenden häufig die Top-Level-Domain „.ai“. In Zeiten der KI ist es viel zu riskant, von Endnutzern zu erwarten, dass sie die Validität einer Website überprüfen.

Nachdem Sie gemeinsam mit Ihrem Unternehmenssicherheitsteam die Bereiche ermittelt haben, in denen KI sinnvoll eingesetzt werden kann, sollten Sie die für Ihre Anforderungen am besten geeigneten Tools auswählen. Dies ist jedoch nur ein Teil der Lösung, da es ebenso wichtig ist, den Zugriff auf andere KI-Tools zu verhindern. Um dieses Ziel zu erreichen, benötigen Sie Einblick in den Browser-Verkehr Ihres Unternehmens.

Nachdem die geeigneten Tools ausgewählt und die Sichtbarkeit hergestellt worden ist, ist es an der Zeit, die Benutzer zu schulen. Eine der einfachsten Möglichkeiten, dies zu tun, besteht darin, Benutzer auf das genehmigte Tool umzuleiten, wenn sie eine als GenAI klassifizierte Website aufrufen. Eine Benachrichtigung kann den Benutzer über die Sicherheitsvorkehrungen der Organisation und den Grund für die Weiterleitung informieren.

Während dieses Zeitraums ist es hilfreich, eine Möglichkeit zu haben, den Web-Datenverkehr genauer zu untersuchen, um sicherzustellen, dass alle Benutzer die Vorschriften einhalten.

[2] TELUS Digital – Umfrage zur digitalen Erfahrung, Februar 2025

[3] AI Gone Wild: Why Shadow AI Is Your IT Team’s Worst Nightmare, Cloud Security Alliance, 4.3.2025

So kann Menlo helfen

Die einfache Lösung für dieses Problem besteht darin, den Zugriff auf als GenAI klassifizierte Sites mithilfe eines Secure Web Gateway (SWG) zu blockieren. Menlo geht noch einen Schritt weiter und leitet Nutzer beim Surfen automatisch zu zugelassenen GenAI-Tools weiter und informiert sie über die Verwendung des neuen Tools mit anpassbaren Bannerseiten. Menlo Browsing Forensics kann so eingestellt werden, dass der gesamte als GenAI kategorisierte Datenverkehr aufgezeichnet wird, und liefert eine videoähnliche Aufzeichnung der gesamten Benutzersitzung.

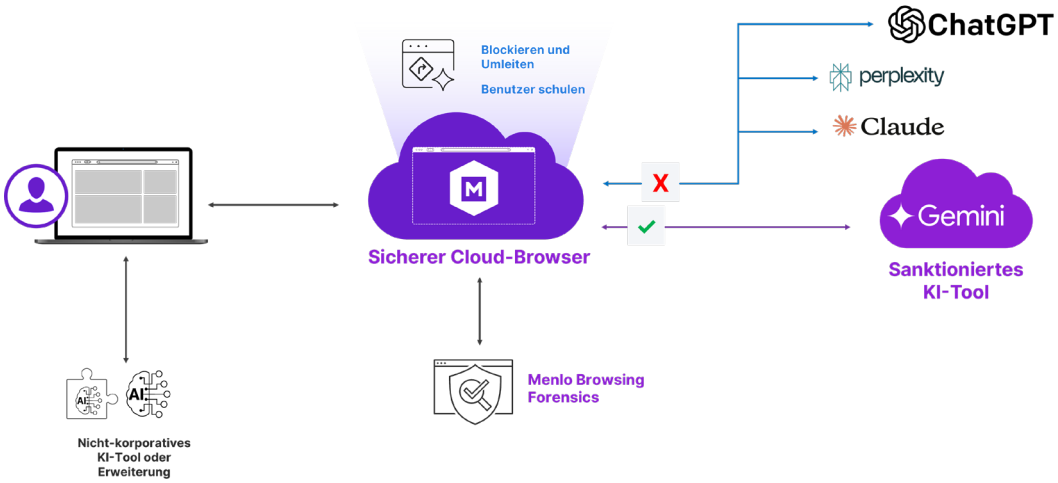

Abbildung 2: Blockieren Sie automatisch den Zugriff auf nicht genehmigte Websites im Menlo Secure Cloud Browser, während Sie die Benutzer schulen. Setzen Sie die Einhaltung der Sichtbarkeit von Menlo Browsing Forensics durch.

Die Realität ist jedoch, dass sich KI als Kategorie so schnell weiterentwickelt, dass kein Klassifizierungssystem wirklich mithalten kann. Deshalb ist es wichtig, über das Tool selbst hinauszugehen, um zu überlegen, welches Benutzerverhalten erlaubt sein sollte, und sicherzustellen, dass Daten automatisch geschützt werden.

Über sanktionierte Tools hinaus zu sanktionierter Nutzung

Ein Großteil der KI-Nutzung, die zu Datenlecks führt, ist wahrscheinlich nicht böswillig, sondern vielmehr ein Versuch der Nutzer, Zeit zu sparen und die Produktivität zu steigern. Diese Situation spiegelt das Szenario einer „Insider-Bedrohung“ wider, über das Menlo bereits berichtet hat.

Sie können die Nutzung von GenAI-Tools schützen, indem Sie dieselben Methoden anwenden, die Sie auch zum Schutz interner Anwendungen vor Insider-Bedrohungen einsetzen würden. Durch die Einstufung von GenAI-Websites als sensible Anwendungen können Sie Daten und Vermögenswerte schützen, indem Sie Inhalte nach Dateityp blockieren und Kopier- und Einfügefunktionen einschränken oder untersagen. Selbst Wasserzeichen sind hilfreich, um die Benutzer für den Umgang mit sensiblen Informationen zu sensibilisieren, mit denen sie möglicherweise arbeiten.

Der Schlüssel hier ist, dass diese Regeln automatisch durchgesetzt werden müssen. Da die meisten Benutzerinteraktionen im Browser stattfinden, ist dies erneut der logische Ort, um solche Durchsetzungen zu integrieren. Indem GenAI wie jede andere Anwendung behandelt wird, die Einschränkungen für eine sichere Nutzung erfordert, lassen sich viele dieser Anforderungen ganz einfach erfüllen.

So kann Menlo helfen

Die Regeln für Menlo-Inhalte, darunter Kopieren/Einfügen, Hochladen/Herunterladen, Wasserzeichen und Zeichenbeschränkungen, können mit nur wenigen Klicks aktiviert werden. Diese Funktion ist in den Menlo Secure Cloud Browser integriert und dient dazu, Benutzer daran zu erinnern, auf Datenlecks zu achten. Die Sichtbarkeit kann über Menlo Browsing Forensics bereitgestellt werden, um die Durchsetzung zu unterstützen.

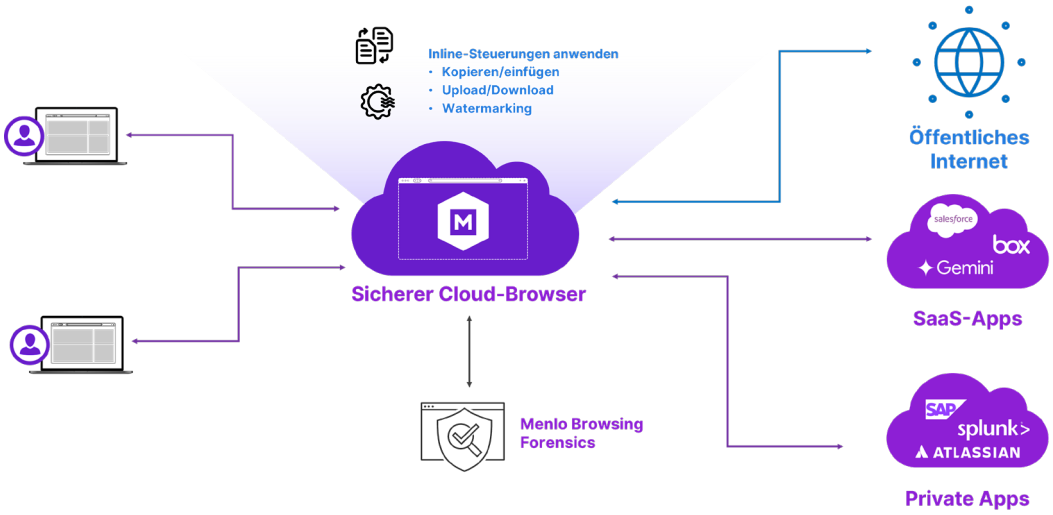

Abbildung 3: Setzen Sie Richtlinien automatisch und inline mit dem Menlo Secure Cloud Browser durch, mit Durchsetzung und Transparenz durch Menlo Browsing Forensics.

Schützen Sie Ihre Daten

Wenn Sie noch keine benutzerfreundlichen DLP-Tools eingeführt und mit deren Durchsetzung begonnen haben, sollten Sie dies unverzüglich tun. Wenn Nutzer Inhalte in GenAI-Tools hochladen, insbesondere in Formaten wie PDF, die häufig interne oder anderweitig sensible Daten enthalten, kann dies katastrophale Folgen haben, selbst wenn die Offenlegung unbeabsichtigt erfolgt. Eine Möglichkeit, diese potenziell sensiblen Dokumente zu schützen, besteht darin, das Hochladen gänzlich zu verbieten. Eine andere Methode besteht darin, DLP-Regeln anzupassen, um vertrauliche Informationen zu kennzeichnen.

So kann Menlo helfen

Menlo bietet über 300 DLP-Wörterbücher, die Sie mit wenigen Klicks auf Inhalte anwenden können. Sie können auch Ihr eigenes Wörterbuch erstellen, um noch individuellere DLP-Steuerungen bereitzustellen. Diese Funktionen sind in den Secure Cloud Browser integriert, was es einfach macht, dort Schutz zu bieten, wo er am wichtigsten ist. Wenn Inhalte, die auf eine GenAI-Site hochgeladen werden, ein DLP-Ereignis auslösen, können Sie den Upload automatisch blockieren oder einfach protokollieren.

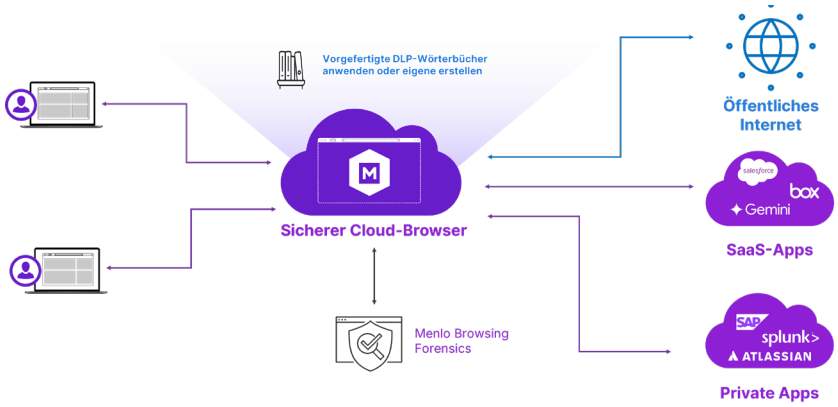

Abbildung 4: Automatische Durchsetzung von DLP-Richtlinien im Einklang mit DLP-Wörterbüchern im Secure Cloud Browser, mit Durchsetzung und Sichtbarkeit durch Menlo Browsing Forensics.

Inhaltsprüfung aktivieren

Wenn Sie sich dafür entscheiden, Downloads von KI zuzulassen, müssen Sie unbedingt sicherstellen, dass die Benutzer keine Malware einschleusen. Die Möglichkeit, Dateien aktiv zu scannen, um festzustellen, dass keine Malware oder schädliche aktive Inhalte enthalten sind, kann zur Sicherheit des Unternehmens beitragen.

So kann Menlo helfen

Der Menlo Secure Cloud Browser überprüft automatisch alle Inhalte, es sei denn, Sie entscheiden sich, ihn zu deaktivieren. Zu den Schutzmaßnahmen gehören Datei-Hash-Prüfungen, Virenschutz und Sandboxing. Sie werden auf alle Inhalte angewendet, einschließlich passwortgeschützter Dateien und Archive. Wenn Inhalte die Überprüfung nicht bestehen, können Sie sie blockieren oder durch Deaktivieren aktiver Inhalte für die Verwendung sicher machen.

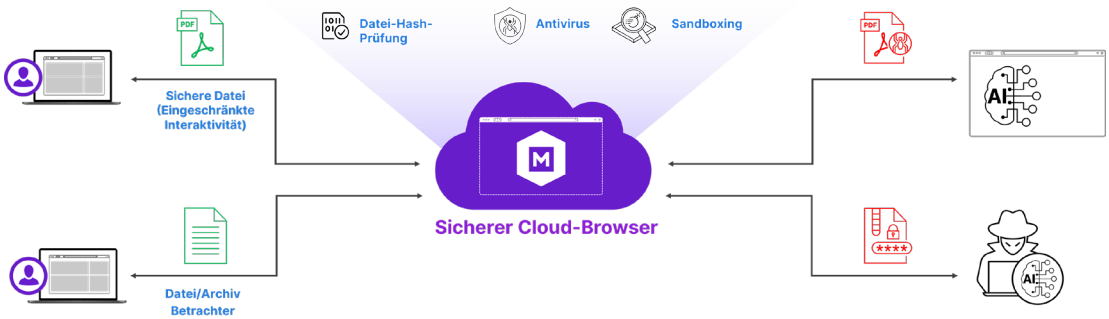

Abbildung 5: Die Inhaltsprüfung erfolgt automatisch und inline, auch für verschlüsselte Dateien und Archive. Inhalte, die die Prüfung nicht bestehen, können blockiert oder als „sicher" eingestuft werden.

Wenn die Beibehaltung der vollen Funktionalität wichtig ist, ist Votiro von Menlo führend in der Kategorie „Content Disarm and Reconstruction“ (Inaktivierung und Rekonstruktion von Inhalten). Sobald eine Verbindung hergestellt ist, werden alle Inhalte automatisch überprüft und bereinigt, es sei denn, die Richtlinien bestimmen etwas anderes.

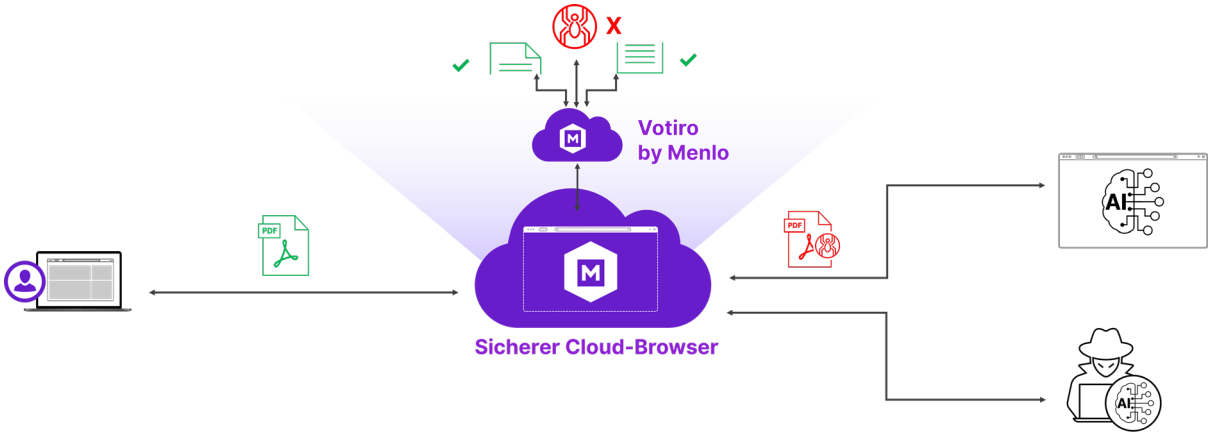

Abbildung 6: Votiro zerlegt Inhalte vollständig, entschärft sie und setzt sie wieder zusammen, sodass sie sowohl voll funktionsfähig als auch sicher sind.

Schützen Sie Ihr Unternehmen vor dem Missbrauch von KI

GenAI hat es Angreifern einfacher denn je gemacht, in Unternehmen Fuß zu fassen. Der Schutz vor gefälschten KI-Tools ist ein guter Grund, eine Richtlinie zur akzeptablen Nutzung einzuführen und durchzusetzen, aber der Schutz muss noch tiefer gehen. Es ist sinnlos, von den Benutzern zu verlangen, dass sie die Aufgabe übernehmen, die heutigen Phishing-Betrugsversuche selbst zu analysieren, da diese Inhalte speziell darauf ausgelegt sind, Legitimität zu vermitteln, und oft durch sorgfältige Recherchen über das Ziel, Deepfake-Inhalte und mehr untermauert werden. Benutzer müssen vor solchen Bedrohungen geschützt werden, und der Schutz muss automatisch sein.

So kann Menlo helfen

Die heutigen Phishing-Angriffe sind gefährlicher als je zuvor. Mit Hilfe von KI können häufige „Anzeichen“ wie schlechte Rechtschreibung oder Grammatikfehler eliminiert werden. Es ist nun möglich, diese Bedrohungen schnell zu iterieren und die Anzahl der Angriffe zu erhöhen, bis etwas die Abwehrmaßnahmen umgeht. Heutige Phishing-Angriffe können über SMS, soziale Netzwerke oder sogar Sprachplattformen erfolgen, sodass herkömmliche Abwehrmaßnahmen, die sich ausschließlich auf E-Mails konzentrieren, nicht mehr ausreichen.

KI hat auch die Entwicklung hochgradig personalisierter Spear-Phishing-Angriffe ermöglicht, bei denen Deepfake-Audio- und -Videodaten mit einer vollständigen Übersicht über das Leben des Ziels kombiniert werden.

Menlo HEAT Shield AI arbeitet automatisch, um diese Bedrohungen in Echtzeit und inline abzufangen, bevor sie den Endpunkt des Benutzers erreichen können, unabhängig von ihrer Quelle. Da HEAT Shield AI nicht auf Signaturen basiert (die nur bereits bekannte Bedrohungen erkennen können), kann es alle Phishing-Angriffe stoppen, selbst solche, die völlig neu sind.

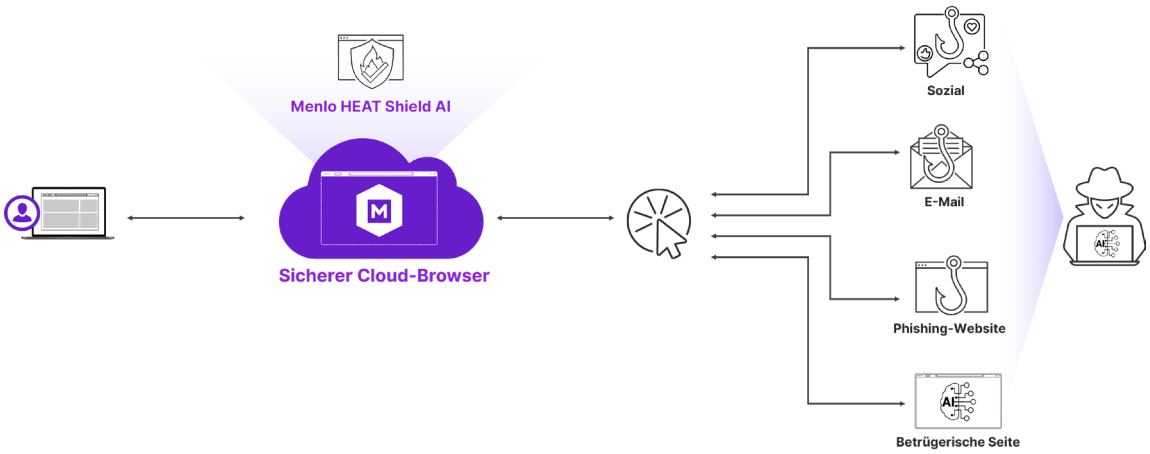

Abbildung 7: Menlo stoppt KI-gesteuerte Bedrohungen mit HEAT Shield AI, das entwickelt wurde, um Highly Evasive Adaptive Threats (HEAT) wie diese zu erkennen und zu stoppen, sobald der Benutzer darauf klickt.

Schützen Sie interne Anwendungen, während Sie Zero-Trust-Zugriff ermöglichen

Es ist von entscheidender Bedeutung, auch die Kehrseite des Datenabflusses aus dem Unternehmen zu berücksichtigen und mögliche Gefahren zu erkennen, die in eingehenden Inhalten stecken, insbesondere bei nicht verwalteten Geräten. Wenn ein Benutzer beispielsweise persönliche Informationen auf eine Lebenslauf-Website hochlädt, kann die zurückgesendete PDF-Datei mehr enthalten als nur ein ansprechendes Layout.

Sie können zwar Schutzmaßnahmen für Ihre Mitarbeiter auf verwalteten Geräten aktivieren und durchsetzen, aber es ist unmöglich, vollständig zu kontrollieren, was auf einem BYOD-Endgerät oder einem Gerät eines Drittanbieters geschieht. Gleichzeitig müssen diese Benutzer auf Ihre sensiblen internen Anwendungen zugreifen können, um ihre Arbeit zu erledigen. Es ist unerlässlich, eine Zero-Trust-Zugriffsmethode bereitzustellen, die Sicherheit und Produktivität vereint.

Wie Menlo helfen kann

Menlo Secure Application Access vereinfacht die Bereitstellung von Zugriffsrechten mit minimalen Berechtigungen für alle Benutzer, selbst wenn das Gerät nicht im Besitz des Unternehmens ist oder von diesem verwaltet wird. Mit Menlo wird jede möglicherweise vorhandene Malware automatisch vom Secure Cloud Browser blockiert, wenn der Benutzer auf interne oder SaaS-Anwendungen zugreift. Mit der zunehmenden Beliebtheit von GenAI steigt auch die Wahrscheinlichkeit, dass Malware auf nicht verwalteten Geräten auftaucht. Mit Menlo können Sie den Zugriff ermöglichen, ohne sich Gedanken über Malware machen zu müssen.

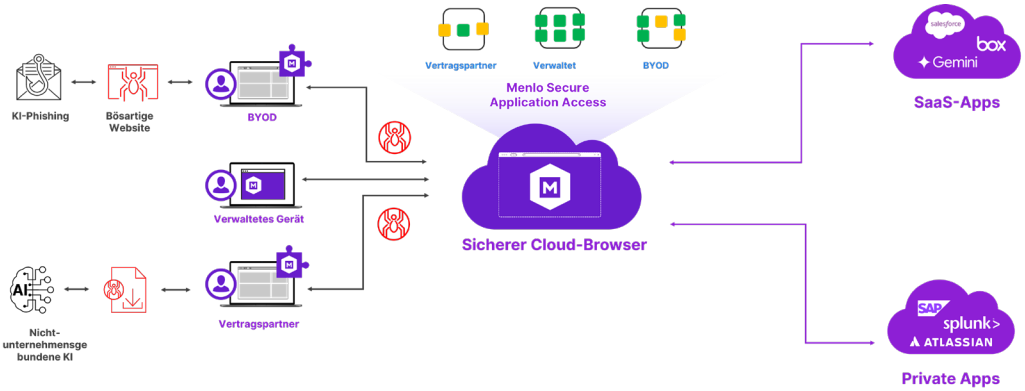

Abbildung 8: Bieten Sie allen Benutzern und allen Geräten Zero-Trust-Zugriff, ohne Ihre internen oder SaaS-Anwendungen zu gefährden.

Vergessen Sie nicht den lokalen Browser

Der Secure Cloud Browser bietet zwar einen umfassenden Schutz, doch die führenden Anbieter von Browsern für Unternehmen, Microsoft Edge und Google Chrome, arbeiten kontinuierlich an Innovationen, was ein wichtiger Grund für ihre anhaltende Beliebtheit ist. Mit dem Menlo Browser Posture Manager können Benutzer ihren eigenen Browsertyp auswählen und diesen sicher verwenden, wodurch eine umfassende Verteidigungsstrategie gewährleistet ist.

Aktuelle Versionen der heutigen Unternehmensbrowser verfügen bereits über KI-Funktionen, und weitere werden folgen. Wie die meisten neuen Funktionen sind diese in der Regel standardmäßig aktiviert. Das bedeutet, dass Sie sich eingehender mit den Richtlinien befassen müssen, um sicherzustellen, dass neue Funktionen im Einklang mit der allgemeinen Sicherheitsstrategie Ihres Unternehmens stehen. Ihr Unternehmen könnte beispielsweise beschließen, die Schreibunterstützung durch GenAI zuzulassen, aber zu verbieten, dass diese Informationen an das öffentliche Modell zurückgegeben werden.

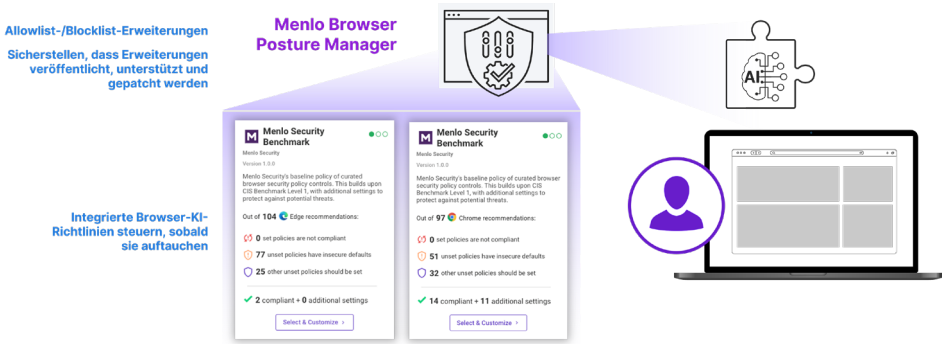

Abbildung 9: Die sichere Nutzung von GenAI muss den lokalen Browser umfassen. Mit dem Menlo Browser Posture Manager lassen sich Richtlinien einfach verwalten und Erweiterungen zulassen oder blockieren, noch bevor Sicherheitsvorschriften zum Tragen kommen.

Zusammenfassung

Menlo ist seit über einem Jahrzehnt im Bereich der Sicherung der weltweit führenden Unternehmensbrowser tätig. Das Unternehmen bietet eine Vielzahl von Sicherheitsfunktionen, mit denen Sie diejenigen aktivieren können, die für Ihr Unternehmen am besten geeignet sind, und diese weiter nach Benutzern oder Gruppen anpassen können. Viele der wichtigsten Elemente für die sichere Nutzung von GenAI sind in die Lösung integriert, werden automatisch und inline angewendet und sind ohne zusätzliche Kosten verfügbar. Alle Funktionen werden über eine einzige Benutzeroberfläche gesteuert, sodass Sie nicht zwischen verschiedenen Verwaltungsbildschirmen hin- und herspringen müssen, um genau das zu erhalten, was Sie benötigen.

Mit Menlo können Sie:

- Sichern Sie den gesamten Webdatenverkehr für alle Benutzer, auch für diejenigen auf nicht verwalteten Geräten.
- Stellen Sie automatisch DLP-Funktionen bereit, darunter Kontrollen für Inhaltsformate und DLP-Regeln, die über mehr als 300 integrierte DLP-Wörterbücher bereitgestellt werden können. Sie können auch Ihr eigenes DLP-Wörterbuch erstellen, um eine noch individuellere Steuerung zu ermöglichen.
- Vollautomatische Inhaltsprüfung, einschließlich Datei-Hash-Prüfungen, Virenschutz und Sandboxing, selbst für passwortgeschützte Dateien und Archive.
- Funktionen zum Entschärfen und Rekonstruieren von Inhalten von Votiro by Menlo.
- HEAT Shield AI schützt vor der wachsenden Bedrohung durch ausweichende, adaptive Phishing-Angriffe.
- Sicherer Anwendungszugriff, der Zero Trust und Zugriff mit geringsten Berechtigungen auf interne Anwendungen für alle autorisierten Benutzer von jedem Gerät aus ermöglicht. Die Inhalte werden durch den Secure Cloud Browser vermittelt, sodass Ihr Unternehmen geschützt bleibt.

GenAI beginnt im Browser. Sichern Sie es dort – mit Menlo Security.

Über Menlo Security

Menlo Security eliminiert ausweichende Bedrohungen und schützt die Produktivität mit dem Menlo Secure Cloud Browser. Menlo erfüllt das Versprechen cloud-basierter Sicherheit und ermöglicht einen Zero-Trust-Zugriff, der einfach zu implementieren ist. Der Menlo Secure Cloud Browser verhindert Angriffe und macht Cyber-Abwehrmaßnahmen für Endbenutzer unsichtbar, während sie online arbeiten, wodurch die Betriebsbelastung der Sicherheitsteams verringert wird.

Menlo schützt Ihre Benutzer und sichert den Zugriff auf Anwendungen und bietet damit eine vollständige Browserlösung für Unternehmen. Mit Menlo können Sie mit einem einzigen Klick Browser-Sicherheitsrichtlinien implementieren, den Zugriff auf SaaS- und private Anwendungen sichern und Unternehmensdaten „bis zur letzten Meile“ schützen. Sichern Sie Ihre digitale Transformation mit zuverlässigem und bewährtem Cyber-Schutz, auf jedem Browser.

Arbeiten Sie sorgenfrei und bringen Sie Ihr Unternehmen mit Menlo Security voran.

Mehr erfahren: https://www.menlosecurity.com
Kontakt: ask@menlosecurity.com