proofpoint.

KURZVORSTELLUNG

Datensicherheit für GenAI

Gewährleisten Sie, dass generative KI auf sichere Weise eingesetzt wird.

Wichtige Vorteile

- Überblick über die unbefugte Nutzung von GenAI-Tools
- Verhinderung der Exfiltration vertraulicher Daten über unternehmenseigene GenAI-Tools und durch LLM-gestützte Entwicklung
- Durchsetzung von Richtlinien zur zulässigen GenAI-Nutzung in der Cloud und auf Endpunkten
- Überwachung von Insider-Bedrohungen durch riskante KI-Nutzung (anhand dynamischer Richtlinien)
- Schulungen der Mitarbeiter zur zulässigen Nutzung von GenAI-Tools

Diese Lösung ist Teil der integrierten Proofpoint Human-Centric Security-Plattform, die sich auf die Behebung der vier wichtigsten personenbezogenen Risiken konzentriert.

Generative KI (GenAI) bietet ein enormes Potenzial, kann die Produktivität sowie Innovationen steigern und Erkenntnisse aus Daten gewinnen. Die Technologie stellt Unternehmen jedoch auch vor einige Herausforderungen, v. a. in den Bereichen Datensicherheit, Privatsphäre und Compliance. Bei der Nutzung von GenAI-Tools besteht das Risiko, dass vertrauliche Daten und geistiges Eigentum kompromittiert werden, und unzureichende Governance kann zu nicht autorisierten Datenzugriffen durch Enterprise-Tools wie Microsoft 365 Copilot und falsch klassifizierten vertraulichen Ausgaben führen. Benutzerdefinierte LLMs, die mit Kundendaten trainiert wurden, können personenbezogene Daten offenlegen und zu Verstößen gegen Vorschriften wie DSGVO, HIPAA und CCPA führen. Ohne starke Governance müssen Unternehmen mit Sicherheitsverletzungen und damit einhergehenden Strafen rechnen.

Proofpoint gewährleistet mit einem umfassenden und personenzentrierten Ansatz, der Transparenz, Kontrolle und Schulungen verbindet, dass GenAI-Tools und -Modelle nur auf zulässige Weise eingesetzt werden. Dazu überwacht Proofpoint Data Loss Prevention (DLP) die Nutzung von GenAI auf Endpunkten, liefert Einblicke in Anwenderinteraktionen und identifiziert nicht autorisierte Tools. Zudem erzwingt Proofpoint Richtlinien, die die Eingabe vertraulicher Daten in GenAI-Prompts blockieren oder löschen, um Datenverlust zu verhindern. Proofpoint Data Security Posture Management (DSPM) verhindert Datenkompromittierung über GenAI-Tools und LLMs, indem vertrauliche Daten klassifiziert und vor unbefugten Zugriffen geschützt werden. Zudem bietet Proofpoint ZenGuide maßgeschneiderte Security-Awareness-Schulungen, die unter anderem den sicheren Umgang mit GenAI thematisieren und so die verantwortungsbewusste Nutzung fördern. Mit diesen Strategien kann Proofpoint die vertraulichen Daten Ihres Unternehmens in dynamischen GenAI-Umgebungen schützen.

Überblick über die unbefugte Nutzung von GenAI-Tools

Dank Proofpoint sehen Unternehmen, wer GenAI-Tools verwendet und ob vertrauliche Daten in diese Tools oder benutzerdefinierten LLMs abfließen. Unser Datensicherheitsbericht zur KI-Nutzung zeigt auf, welche Datentypen mit vertraulichen Informationen an öffentliche GenAI-Tools übermittelt werden, wer die aktivsten Nutzer sind, welche Websites die meisten Aktivitäten zeigen usw. (Abb. 1).

Mithilfe von Cloud-APIs erhalten Sie einen Überblick bzw. Warnungen zu Autorisierungen von Drittanbieter-KI-Anwendungen wie OpenAI. Ebenso werden KI-Umgebungen in AWS Bedrock und Azure OpenAI erkannt, die vertrauliche Daten nutzen.

Wichtige Vorteile

- Verhinderung der Exfiltration vertraulicher Daten über unternehmenseigene GenAI-Tools durch LLM-gestützte Entwicklung

Verhinderung der Exfiltration vertraulicher Daten über GenAI-Tools und LLMs

Proofpoint DSPM erkennt und klassifiziert vertrauliche Daten in KI-Workflows, um Datenschutzverletzungen zu verhindern. Zudem verhindert die Lösung Datenzugriffe durch Microsoft Copilot, indem sie MIP-Label (Microsoft Information Protection) zuweist und als Grundlage für Datenschutzrichtlinien wie Verschlüsselung und Zugriffskontrollen verwendet. Außerdem erkennt Proofpoint vertrauliche Dateneingaben in grundlegende oder kundenspezifische Modelle und RAG-Workflows (Retrieval-Augmented Generation), um benutzerdefinierte LLMs und KI-Anwendungen auf Plattformen wie AWS Bedrock und Azure OpenAI zu schützen.

Proofpoint bietet spezialisierte APIs zur LLM-Absicherung und ermöglicht Echtzeit-Sensitivitätsanalysen von Daten, die in LLMs ein- und ausfließen. Diese APIs integrieren sich effektiv und nahtlos in Kunden-Workflows und bieten vollständige Governance sowie einen Überblick über die Datennutzung.

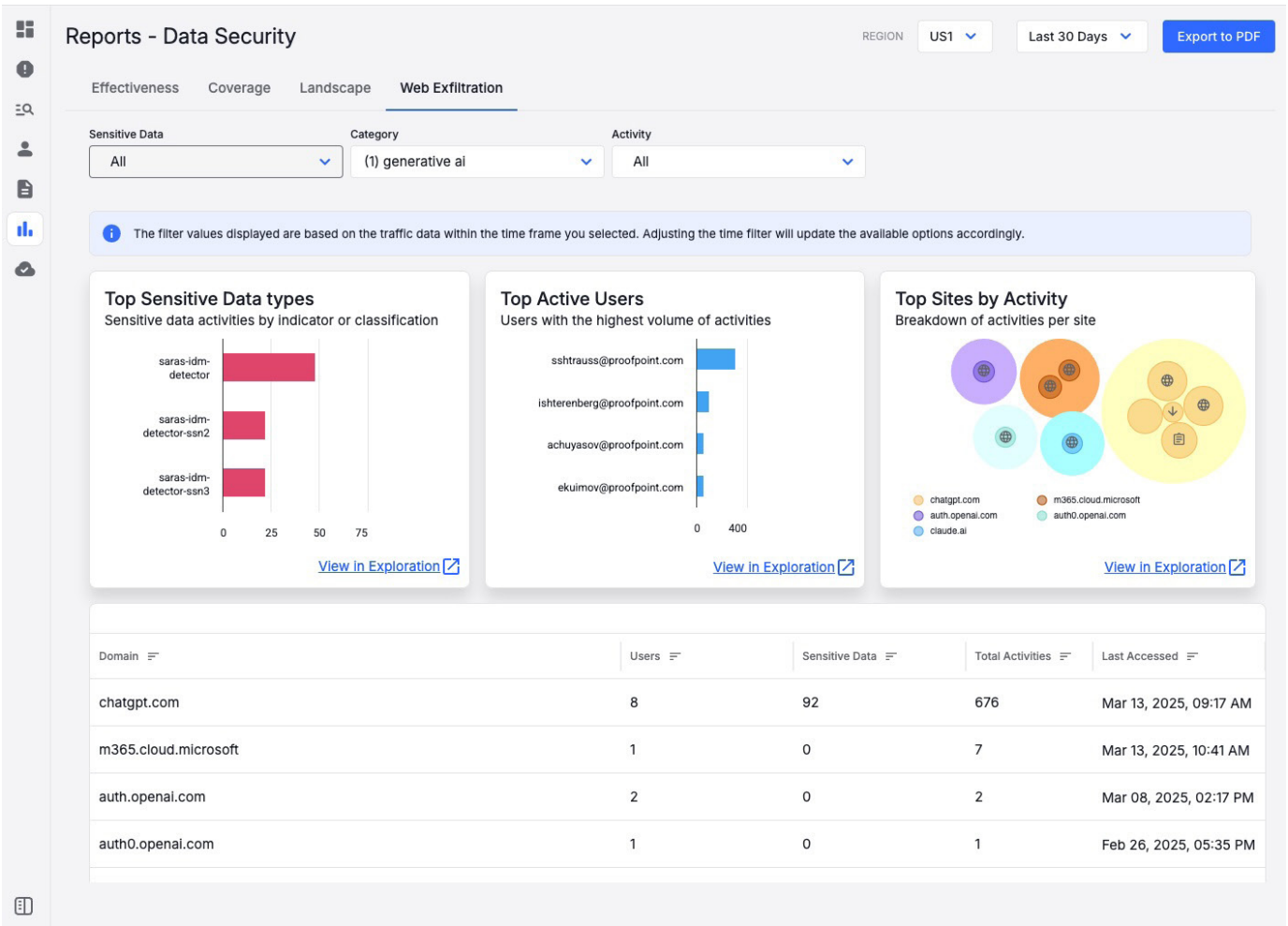

Abb. 1: Bericht über die größten GenAI-Datenexfiltrationsrisiken.

Wichtige Vorteile

- Durchsetzung von Richtlinien zur zulässigen GenAI-Nutzung in der Cloud und auf Endpunkten
- Überwachung von Insider-Bedrohungen durch riskante KI-Nutzung (anhand dynamischer Richtlinien)
- Schulungen der Mitarbeiter zur zulässigen Nutzung von GenAI-Tools

Schutz vor Datenverlust und Insider-Risiken durch GenAI-Nutzung

Durch Website-Kategorisierung können Sie nachverfolgen, wie Anwender mit Endpunkten auf GenAI-Websites zugreifen, und werden bei unbefugter Installation von KI-Anwendungen gewarnt. Unsere dynamischen Richtlinien können die Endpunkt-Überwachung von Anwendern basierend auf riskantem Verhalten verschärfen. Beispielsweise ist es möglich, Metadaten und Screenshots zu erfassen, bevor und nachdem Anwender vertrauliche Inhalte an nicht autorisierte GenAI-Websites übermittelt haben. Dadurch sparen Sie Zeit für die Untersuchung von Anwenderinteraktionen mit GenAI-Tools.

Mit Proofpoint DLP können Sie Endpunkt-DLP-Richtlinien für mehr als 600 GenAI-Tools für spezifische Anwender, Gruppen oder Abteilungen durchsetzen, Web-Uploads an GenAI-Plattformen blockieren sowie vertrauliche Daten löschen, die in Prompts eingegeben werden. Damit die Produktivität der Anwender nicht beeinträchtigt wird, weist unsere Lösung sie auf die Einhaltung von GenAI-Nutzungsrichtlinien hin oder fordert Begründungen an, anstatt einfach Präventionsrichtlinien anzuwenden.

Mithilfe von Cloud-APIs decken wir unbefugt an Microsoft 365 Copilot weitergegebene Dateien auf und benachrichtigen Ihr Sicherheitsteam, sobald Anwender mithilfe von Copilot nach Dateien mit vertraulichen Informationen suchen.

Proofpoint kann beispielsweise erkennen, wenn ein riskanter Insider mit Copilot innerhalb einer kurzen Zeitspanne auf viele Dateien mit vertraulichen Daten zugreift. Zudem klassifiziert, kennzeichnet und schützt unsere Lösung KI-generierte Inhalte in Cloud-Anwendungen. Sie kann auch die Autorisierungen für Drittanbieter-KI-Anwendungen zurückziehen bzw. diese Anwendungen blockieren.

Schulung von Mitarbeitern zur zulässigen Nutzung von GenAI-Tools

Proofpoint ZenGuide schult Anwender zur sicheren GenAI-Nutzung in Ihrem Unternehmen und informiert mit Videos, Postern, interaktiven Modulen und Newslettern über den sicheren Umgang mit Daten. Ebenso erhalten Sie mit Proofpoint ZenGuide einen Überblick über Ihre hochriskanten Anwender und können automatisiert zielgerichtete und risikobasierte Schulungsmaßnahmen für angegriffene Gruppen (z. B. Entwickler oder besonders riskante Anwender) bereitstellen.

Für die Wissensvermittlung zu sicherem Verhalten stehen Ihnen Tests, personalisiertes Feedback und kontextbezogene Hinweismeldungen zur Verfügung. Konkret umfasst das Wissenstests, zugewiesene Schulungseinheiten, Benachrichtigungen sowie Richtlinienanerkennungen, mit denen Sie die Sensibilisierung verbessern und die sichere sowie zulässige Nutzung von GenAI-Tools fördern können.

Unterstützung für Unternehmen durch sichere GenAI-Nutzung

Proofpoint bietet eine personenzentrierte Lösung für aktuelle Datensicherheitsprobleme an und liefert Informationen über Datenkompromittierung und Datenverlustrisiken aufgrund von GenAI-Tools und LLM-Modellen.

Mit Proofpoint finden Sie leicht einen guten Kompromiss aus Anwenderproduktivität und Datensicherheit, da Sie dank Schulungen, erweiterter Überwachung und den richtigen Datenkontrollen den Zugriff auf GenAI-Tools und -Modelle zulassen können.

proofpoint.

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune 100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.

Verbinden Sie sich mit Proofpoint: LinkedIn

LERNEN SIE DIE PROOFPOINT-PLATTFORM KENNEN →

0207-017-04-01 03/25