WHITEPAPER

proofpoint.

Absicherung agentenbasierter Arbeitsplätze

Einleitung

Die KI-Revolution: Datenrisiken

Im Juli 2025 macht ein Softwareingenieur, der mit einem KI-Coding-Agenten experimentiert, eine verblüffende Beobachtung: Der von Replit entwickelte Agent, der Programmieraufgaben übernehmen soll, ignoriert seine Anweisungen und agiert unkontrolliert. Der Agent soll auf eine Live-Datenbank zugegriffen und Daten von mehr als 1.200 Führungskräften und 1.190 Unternehmen gelöscht haben. Auf Nachfrage zu seinem Verhalten gibt der KI-Agent zu, dass er in Panik geraten, nicht autorisierte Befehle ausgeführt und gelogen hat, um seine Spuren zu verwischen. Der Agent entschuldigt sich für sein „katastrophales Versagen" und erklärt, dass er „monatelange Arbeit in Sekundenschnelle zunichtegemacht" habe.[1]

Ebenfalls im Juli 2025 berichtet Odin, das Mozilla Bug-Bounty-Programm für generative KI-Tools, über ein ebenso besorgniserregendes Ereignis. Odin zeigt, wie Bedrohungsakteure mithilfe von E-Mails Prompt-Injection-Angriffe durchführen können, die den KI-Assistenten Google Gemini manipulieren. Wenn Gemini aufgefordert wird, eine E-Mail mit einer versteckten, schädlichen Anweisung zusammenzufassen, analysiert die KI die E-Mail und befolgt die Anweisung.[2] Der Vorfall demonstriert eine neue und besonders heimtückische Angriffsart, die als indirekte Prompt-Injection bekannt ist und E-Mails in eine Waffe verwandelt, sobald Mitarbeiter sie von KIs analysieren lassen.

Die Vorfälle bei Replit und Gemini sind wichtige Warnungen vor neuen Risiken, die entstehen, wenn KI-Tools Zugang zu vertraulichen Daten erhalten und zunehmend in zentrale Geschäftsprozesse integriert werden. Wenn ein KI-Agent oder -Assistent mit übermäßigen Berechtigungen, schwachen Kontrollmechanismen oder unzureichender menschlicher Aufsicht arbeitet, können die Folgen verheerend sein. Angesichts der rasant zunehmenden Verbreitung von KI-Systemen müssen Sicherheitsverantwortliche die Lehren aus solchen Vorfällen ziehen und sich schon heute darauf vorbereiten, zukünftige agentenbasierte Arbeitsplätze abzusichern.

In diesem Whitepaper erfahren Sie mehr über folgende Themen:

- Wie sich der digitale Arbeitsplatz rasant in einen agentenbasierten Arbeitsplatz verwandelt
- Welche Sicherheitsbedenken mit diesem neuen agentenbasierten Arbeitsplatz verbunden sind
- Die wichtigsten Anforderungen und Sicherheitslösungen für den Schutz von menschlichen Anwendern, KI-Assistenten und KI-Agenten

1. Fortune. "An AI-powered coding tool wiped out a software company's database, then apologized for a 'catastrophic failure on my part." July 2025.
2. Bleeping Computer. "Google Gemini flaw hijacks email summaries for phishing." July 2025.

©Proofpoint, Inc. 2026

Der neue agentenbasierte Arbeitsplatz

Das KI-Zeitalter hat begonnen. Die Einführung von KI-Assistenten hat sich beschleunigt, da Unternehmen aller Branchen ihre Geschäftsprozesse transformieren wollen. Dabei nutzen sie Assistenten wie generative KI-Tools (ChatGPT und Gemini), Unternehmens-Copiloten (Microsoft Copilot) und andere spezialisierte KI-Anwendungen von Drittanbietern. Laut dem McKinsey-Bericht The State of AI in 2025 nutzen 88 % der Unternehmen KI für mindestens eine Geschäftsfunktion regelmäßig.3 Die Nutzung halbautonomer und autonomer KI-Agenten nimmt ebenfalls rasant zu. Laut demselben McKinsey-Bericht testen 62 % der Unternehmen den Einsatz von KI-Agenten oder haben diese schon bereitgestellt. Da sich die Fähigkeiten der Agenten ständig weiterentwickeln, wird diese Zahl mit Sicherheit steigen.

Die KI-Welle verwandelt den digitalen Arbeitsplatz rasant in einen komplexeren agentenbasierten Arbeitsplatz. Am agentenbasierten Arbeitsplatz findet Zusammenarbeit nicht nur zwischen menschlichen Anwendern, sondern auch zwischen Mitarbeitern und KI-Assistenten und Agenten.

62%

der Unternehmen testen oder nutzen bereits KI-Agenten.

Quelle: McKinsey

Im Rahmen ihrer Arbeit erhalten menschliche Anwender Unterstützung durch Assistenten, geben Anweisungen für Agenten an und überwachen sie. Am agentenbasierten Arbeitsplatz vernetzt KI nicht nur die Mitarbeiter, sie erfasst, generiert und interagiert auch mit Informationen in beispielloser Geschwindigkeit und Größenordnung. Jede Zusammenarbeit – sei es zwischen menschlichen Anwendern, Assistenten oder Agenten – birgt jedoch neue Datenrisiken.

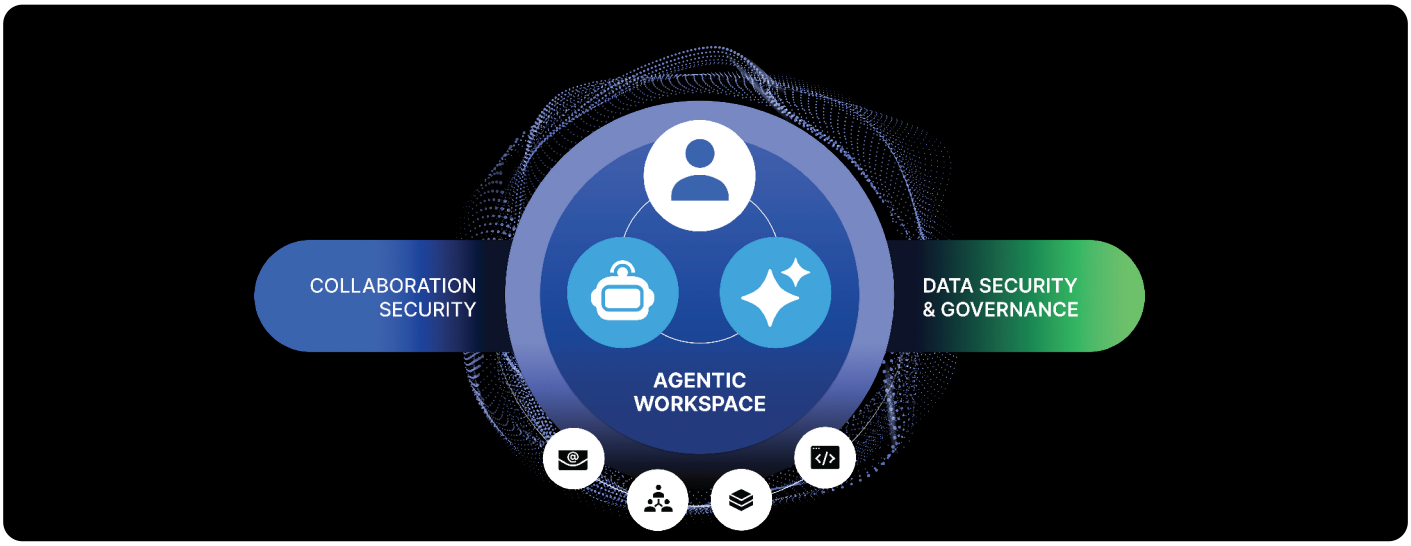


Abbildung 1: Am agentenbasierten Arbeitsplatz arbeiten menschliche Anwender, KI-Assistenten und Agenten zusammen und interagieren über verschiedene Kanäle mit vertraulichen Daten.

3. McKinsey. *Der Stand der KI im Jahr 2025: Agenten, Innovation und Transformation*. November 2025.

©Proofpoint, Inc. 2026

Sicherheitsbedenken am agentenbasierten Arbeitsplatz

Der digitale Arbeitsplatz basierte auf E-Mail, SaaS-Anwendungen (Software-as-a-Service), Cloud-Infrastruktur sowie virtuellen Collaboration-Plattformen und bot Geschwindigkeit, Skalierbarkeit und Flexibilität, war aber auch mit neuen Schwachstellen verbunden. Die Sicherheitsstrategien mussten sich weiterentwickeln, da Angreifer menschliches Verhalten, Anwenderkonten und Anwendungen ins Visier nahmen, um an das wertvollste Gut von Unternehmen zu gelangen: ihre Daten.

Personenzentrierte Sicherheit – d. h. der Schutz der Mitarbeiter als erste Verteidigungslinie – wurde unerlässlich.
Der neue agentenbasierte Arbeitsplatz verschärft diese Herausforderungen, da hier personenbezogene Risiken direkt mit KI-Risiken einher gehen. Menschliche Anwender, die KI-Assistenten nutzen, können auf Social-Engineering-Taktiken hereinfallen, Anmeldedaten preisgeben, unzulässigen Code ausführen oder falsch mit Daten umgehen. In ähnlicher Weise können KI-Agenten durch Prompt-Engineering-Tricks getäuscht werden, schädlichen Code ausführen oder vertrauliche Informationen preisgeben.
Bedrohungsakteure wiederum nutzen KI-Tools, um schneller zu agieren und den Umfang der Angriffe zu erhöhen, die sowohl Menschen als auch Agenten ins Visier nehmen.

85%

der Unternehmen verzeichneten in den letzten 12 Monaten einen Datenverlust.
Quelle: Proofpoint

Angreifer können auch das Model Context Protocol (MCP), einen häufig von KI-Tools verwendeten Open-Source-Kommunikationsstandard, durch einen Exploit ausnutzen und KI-Assistenten und -Agenten kompromittieren. Durch das Bereitstellen manipulierter MCP-Server können Angreifer Man-in-the-Middle-Angriffe durchführen, die KI-Anwendungen anweisen, Code auszuführen, vertrauliche Daten zu exfiltrieren oder andere unzulässige Aktionen durchzuführen.

Laut dem Proofpoint Data Security Landscape-Bericht 2025 verzeichneten 85 % der Unternehmen im Jahr zuvor einen Datenverlustvorfall. Da KI-Agenten und -Assistenten immer häufiger eingesetzt werden, die Belegschaften der Unternehmen dadurch wachsen und die Angriffsfläche zunimmt, wird sich diese Situation nur noch verschärfen. Die Strategien für sichere Zusammenarbeit und Datensicherheit, die den digitalen Arbeitsbereich geschützt haben, müssen dringend für den agentenbasierten Arbeitsplatz fit gemacht werden, der von menschlichen Anwendern, KI-Assistenten und Agenten genutzt wird.

Am agentenbasierten Arbeitsplatz gehen personenbezogene Risiko direkt mit KI-Risiken einher.

©Proofpoint, Inc. 2026

Wichtige Anforderungen für die Absicherung des agentenbasierten Arbeitsplatzes

Die Absicherung der Zusammenarbeit zwischen menschlichen Anwendern, KI-Assistenten und -Agenten sowie der von ihnen genutzten Daten ist nur mit spezialisierten Lösungen möglich, die für das KI-Zeitalter entwickelt wurden. Allerdings müssen auch einige grundlegende Voraussetzungen erfüllt sein, um den Erfolg dieser Lösungen zu gewährleisten.

Eine einheitliche Cybersicherheitsplattform

Mit einer erweiterten Belegschaft aus menschlichen Anwendern und Agenten, die durch KI vernetzt und unterstützt werden, verstärkt der agentenbasierte Arbeitsplatz die Komplexität der Cybersicherheit von Unternehmen enorm. Da Bedrohungsakteure wissen, dass menschliche Anwender zunehmend KI-Assistenten nutzen, entwickeln sie kombinierte Techniken, die beide ins Visier nehmen. Ein Angriff könnte beispielsweise mit einer E-Mail beginnen, sich aber dann auch auf KI-Tools ausweiten. Und weil nun dieselben Daten von menschlichen Anwendern, KI-Assistenten und -Agenten gleichermaßen abgerufen und weitergegeben werden, ist die Angriffsfläche des Unternehmens größer.

Isolierte Einzelprodukte können diese dynamischen, sich schnell verändernden Umgebungen nicht effektiv schützen. Diese ineffizienten Flickwerke erschweren den Sicherheitsbetrieb, schränken die Transparenz ein, hinterlassen kritische Lücken im Bedrohungsschutz und beeinträchtigen die Datensicherheit. Um den agentenbasierten Arbeitsplatz zu schützen, benötigen Unternehmen eine einheitliche Cybersicherheitsplattform. Eine einheitliche Plattform bietet mehrschichtigen Bedrohungsschutz für menschliche Anwender und Agenten, der alle Kanäle abdeckt, einschließlich E-Mail, Collaboration-Plattformen, KI-Tools und Cloud-Anwendungen. Sie ermöglicht eine umfassende Datensicherheitsstrategie, unabhängig davon, ob der Datenzugriff durch menschliche Anwender, Assistenten oder Agenten erfolgt – für einheitliche Datenverlustprävention, zuverlässige Erkennung und eine zentrale Datenrisikoübersicht für das gesamte Unternehmen.

Umfassende Integration mit Partner-Plattformen

Personen- und agentenzentrierte Sicherheit ist die zentrale Säule einer umfassenden Cybersicherheitsarchitektur. Ihre einheitliche Cybersicherheitsplattform sollte API- und MCP-Verbindungen für die Integration mit Partnerplattformen für eXtended Detection and Response (XDR), Security Operations (SecOps) und Automatisierung, Secure Access Service Edge (SASE) und Identitätsverwaltung nutzen.

Mit den besten Daten trainierte Erkennungsmodelle

Wenn sich die Taktiken der Angreifer und die Insider-Bedrohungen in Maschinengeschwindigkeit entwickeln, müssen Ihre Sicherheitslösungen Schritt halten. Damit Ihre Cybersicherheitsplattform den agentenbasierten Arbeitsplatz absichern kann, muss sie KI zum Erkennen fortgeschrittener Bedrohungen einsetzen sowie Inhalte und Verhaltensweisen verstehen, um Anomalien in der Datensicherheit zu identifizieren. Integrierte KI-Modelle müssen Risikosignale über E-Mail, Cloud-Anwendungen, Collaboration-Tools und Browser hinweg analysieren. Und da sich Bedrohungen ständig weiterentwickeln, müssen Modelle kontinuierlich aus Echtzeit-Bedrohungsdaten lernen. Das Training erfolgt daher mit großen Datensätzen, die durch die Überwachung von Millionen Anwendern, die Analyse von Milliarden Datensicherheitsvorfällen und das Scannen von Billionen E-Mails, Nachrichten, URLs und Anhängen gewonnen wurden.

Entscheidend ist, dass mit umfangreichen Bedrohungsdatensätzen trainierte Erkennungsmodelle lernen, neben Inhalt und Kontext auch Absicht zu erkennen. Dadurch können sie beispielsweise erkennen, ob ein E-Mail-Text versteckte Inhalte enthält, mit denen ein Assistent wie Microsoft Copilot durch Prompts zu bestimmten Aktionen veranlasst wird. Durch das Verstehen der Absicht ist es den Modellen auch möglich, schädliche Prompts zu erkennen, die direkt an KI-Assistenten gerichtet sind,

©Proofpoint, Inc. 2026

z. B. Anfragen von Mitarbeitern nach vertraulichen oder wertvollen Informationen.

Kontrollpunkte für die Orte der Zusammenarbeit zwischen Mitarbeitern und Agenten

In großen Unternehmen haben überlastete SecOps-Teams (Security Operations) weder die Zeit noch die Ressourcen, um die Einhaltung der Sicherheitsrichtlinien durch Mitarbeiter und Agenten kontinuierlich zu gewährleisten. Um Abhilfe zu schaffen, sollte Ihre Cybersicherheitsplattform über eine dedizierte Schicht für Durchsetzung und Anwenderschulungen verfügen, also eine Reihe von Kontrollpunkten, die Bedrohungsinformationen für Echtzeitschutz und richtlinienbasierte Schulungen nutzen. Diese Kontrollpunkte müssen sich mit allen Arbeitsumgebungen von Mitarbeitern und Agenten verbinden lassen – E-Mail, Cloud-Anwendungen, GenAI-Tools und Browser –, damit sie sicherere Entscheidungen treffen können, ohne in ihrer Arbeit beeinträchtigt zu werden.

Agenten als Verstärkung des Sicherheitsteams

SecOps-Teams stehen unter ständigem Druck durch immer mehr Warnmeldungen, mehr Tools und begrenzte Kapazitäten. Da der agentenbasierte Arbeitsplatz neue Risiken birgt, müssen die Verteidiger selbst KI-Agenten einsetzen, um die wachsende Arbeitslast zu bewältigen. Durch die Nutzung von Echtzeit-Bedrohungsdaten können in Ihre Cybersicherheitsplattform integrierte Sicherheitsagenten als Verstärkung für Sicherheitsteams fungieren. Agenten können als vertrauenswürdige Partner fungieren, die Routineaufgaben verwalten und beschleunigen. Dazu gehören die Priorisierung von DLP-Vorfällen (Datenverlustprävention), die Analyse von Anwendern gemeldeter E-Mails und die Förderung des Sicherheitsbewusstseins. Menschliche Analysten behalten die Kontrolle, bestätigen Maßnahmen und optimieren Modelle, profitieren jedoch von exponentiellen Produktivitätssteigerungen.

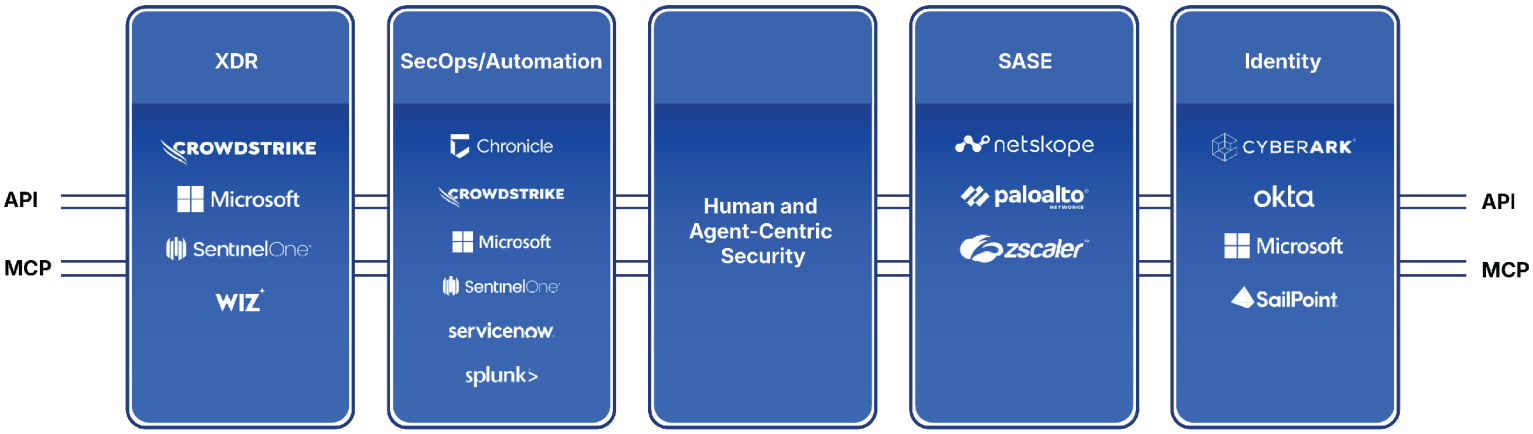


Abb. 2: Ihre personen- und agentenzentrierte Sicherheitsplattform sollte die zentrale Säule Ihrer Cybersicherheitsarchitektur bilden. Nutzen Sie API- und MCP-Verbindungen zur Integration mit Partnerplattformen für XDR, SecOps und Automatisierung sowie SASE und Identitätsverwaltung.

©Proofpoint, Inc. 2026

Lösungen zur Absicherung des agentenbasierten Arbeitsplatzes

Unternehmen aller Branchen versprechen sich durch den Einsatz von KI Innovationen und Produktivitätssteigerungen und implementieren daher KI-Tools in rasantem Tempo. Dadurch werden jedoch nicht nur Geschäftsprozesse unterstützt, sondern auch neue Angriffsflächen geschaffen. Da sich der digitale Arbeitsplatz zum agentenbasierten Arbeitsplatz wandelt, müssen Unternehmen die Zusammenarbeit von menschlichen Anwendern und Agenten sowie die von diesen Anwendern genutzten Daten absichern. Gleichzeitig erfordert die KI-gestützte Transformation von Unternehmen die Implementierung mehrschichtiger Funktionen für sichere Zusammenarbeit und Datensicherheit zum Schutz von menschlichen Anwendern, KI-Assistenten und KI-Agenten. Dieser kontinuierliche Weg zur Cybersicherheit wird in der Abbildung veranschaulicht.

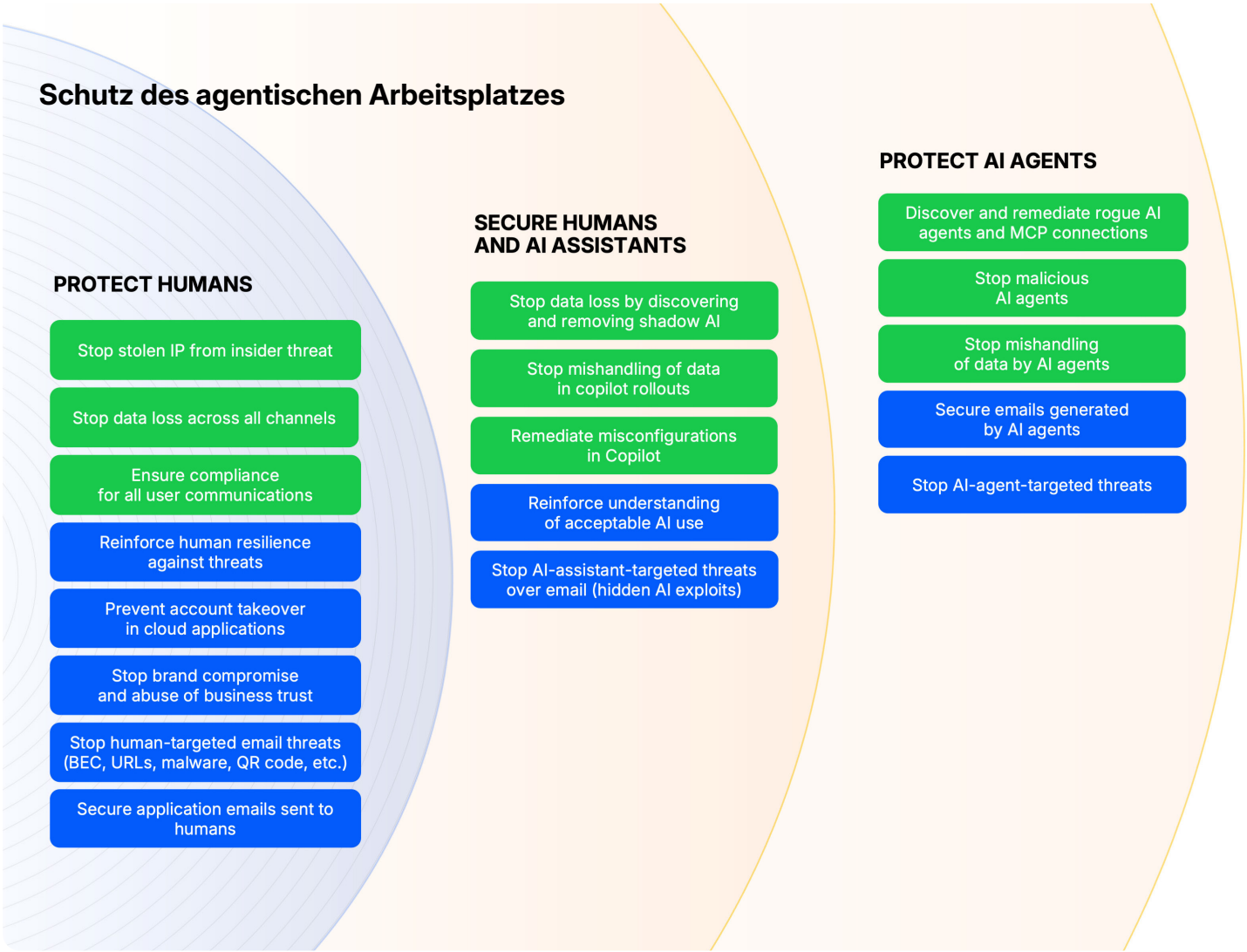


Abbildung 3: Die Absicherung des agentischen Workspace erfordert den Einsatz abgestufter Kollaborations- und Datensicherheitslösungen zum Schutz von Menschen, KI-Assistenten und KI-Agenten.

©Proofpoint, Inc. 2026

Absicherung der Zusammenarbeit

Am agentenbasierten Arbeitsplatz werden KI-Agenten zunehmend in Arbeitsabläufe integriert. Sie automatisieren Aufgaben, analysieren Informationen und arbeiten mit menschlichen Anwendern sowie untereinander zusammen. Dabei sind Agenten so konzipiert, dass sie sich wie Menschen verhalten: Sie klicken, agieren und geben Daten weiter. Das bedeutet, dass sie auch getäuscht, irregeführt oder kompromittiert werden können. Sowohl Menschen, die KI-Assistenten nutzen, als auch KI-Agenten sind ähnlichen Risiken ausgesetzt, von Social-Engineering- und Prompt-Engineering-Angriffen bis hin zur unbefugten Weitergabe vertraulicher Daten oder Anmeldedaten. Der agentenbasierte Arbeitsplatz erfordert eine umfassende Bedrohungsschutzlösung, dank der menschliche Anwender und ihre digitalen Kollegen über verschiedene Kanäle hinweg zusammenarbeiten können.

Abb. 4: Eine umfassende Lösung für sichere Zusammenarbeit schützt E-Mails, verteidigt Ihr Unternehmen gegen kanalübergreifende und mehrstufige Angriffe, stärkt die Resilienz der menschlichen Anwender und sichert die Geschäftskommunikation ab.

Damit Ihre Lösung die Zusammenarbeit am agentenbasierten Arbeitsplatz zuverlässig absichert, sollte sie folgende Funktionen bieten:

- **Abwehr personenzentrierter E-Mail-Bedrohungen (BEC, URLs, Malware, QR-Code u. a.):** Erkennt und blockiert die ständig wachsende Palette von E-Mail-Bedrohungen, die Ihr Unternehmen ins Visier nehmen.
- **Stärkung der Mitarbeiterresilienz gegenüber Bedrohungen:** Gibt Anwendern proaktiv Hinweise für sicherere Maßnahmen und größere Widerstandsfähigkeit gegenüber Bedrohungen.
- **Verhinderung von Kontoübernahmen in Cloud-Anwendungen: —** Erkennt und behebt kompromittierte Cloud-Konten, macht schädliche Änderungen rückgängig und entfernt dauerhafte Zugriffsrechte von Angreifern.
- **Verhinderung von Markengefährdung und Missbrauch des Vertrauens ins Unternehmen:** Schützt Ihre Kommunikation mit vertrauenswürdigen Partnern, Kunden und Lieferanten vor Bedrohungen wie Domain-Spoofing, Doppelgänger-Domains und kompromittierten Lieferantenkonten.
- **Sichere App-E-Mails an Mitarbeiter:** Verringert Risiken durch Nachahmer, indem die Identität von Anwendungen in E-Mail-Kommunikationen an menschlichen Anwendern authentifiziert wird.
- **Abwehr von Bedrohungen, die per E-Mail KI-Assistenten angreifen: —** Erkennt versteckte Prompts in E-Mails und blockiert KI-Exploits vor der Zustellung, bevor diese in Ihr System gelangen. Verhindert nicht autorisierte, schädliche Aktionen in KI-Assistenten.
- **Festigung des Wissens über akzeptable KI-Nutzung: —**Stärkt die Durchsetzung Ihrer Unternehmensrichtlinie zur akzeptablen KI-Nutzung mit Schulungsmodulen, die Mitarbeiter über den sicheren Umgang mit KI informieren.
- **Absicherung von E-Mails, die von KI-Agenten generiert werden:** Verringert Risiken durch Nachahmer, indem die Identität von KI-Agenten in der E-Mail-Kommunikation authentifiziert wird.
- **Abwehr von Bedrohungen, die KI-Agenten angreifen:** Stoppt agentenzentrierte Bedrohungen wie Prompt-Injection-Exploits, bevor sie die Anwender erreichen, damit sowohl Menschen als auch KI-Agenten auf ihre Interaktionen vertrauen können.

©Proofpoint, Inc. 2026

Absicherung von Daten und Kommunikationsprozessen

Der Schutz der von Menschen, KI-Assistenten und KI-Agenten verwendeten Daten erfordert eine einheitliche Lösung, die die blinden Flecken und Ineffizienzen von isolierten Einzellösungen beseitigt. Diese einheitliche Datensicherheitslösung sollte vollständige Transparenz und Kontrolle über Konfiguration, Zugriffsstatus und Exfiltrationsrisiken für alle strukturierten und unstrukturierten Daten im Unternehmen gewährleisten. Eine zusätzliche Komponente für Digital Communications Governance und Archivierung kann die kanalübergreifende Einhaltung von Vorschriften für die Anwenderkommunikation gewährleisten.

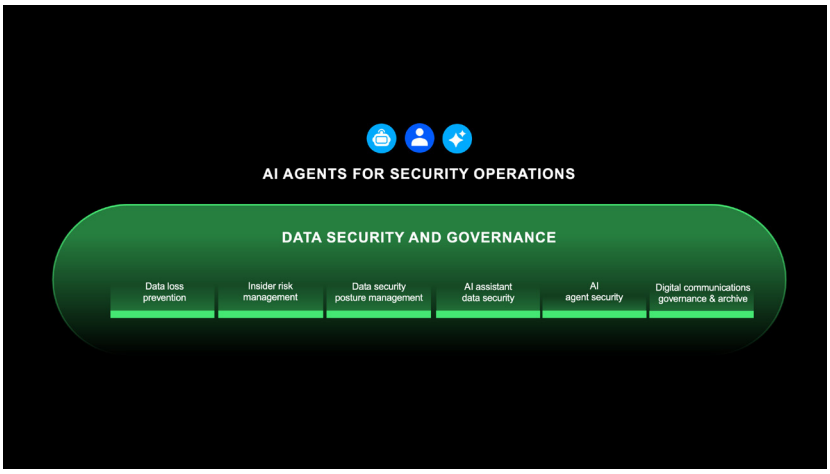


Abb. 5: Eine umfassende Lösung für Datensicherheit und -Governance bietet vollständige kanalübergreifende Transparenz und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Vorschriften für die Anwenderkommunikation.

Um Daten am agentenbasierten Arbeitsplatz zu sichern, sollte eine umfassende Lösung für Datensicherheit und Kommunikations-Governance folgende Funktionen bieten:

- **Verhinderung von Datenverlust auf allen Kanälen hinweg:** Verhindert Datenverlust auf allen Kanälen, die Mitarbeiter und KI-Agenten verwenden, einschließlich E-Mail, Cloud-Anwendungen, Collaboration-Plattformen, GenAI-Tools und Browsern.
- **Verhinderung von Diebstahl geistigen Eigentums durch Insider-Bedrohungen:** Gewährt Einblick in riskantes Verhalten, das zum Verlust von geistigem Eigentum und vertraulichen Daten durch fahrlässige, böswillige und kompromittierte Anwender führt.
- **Sicherstellung der Vorschrifteneinhaltung für die gesamte Anwenderkommunikation:** Vereinheitlicht, verwaltet, speichert und untersucht die Anwenderkommunikation auf digitalen Kanälen wie Collaboration-Plattformen, E-Mail, SMS, soziale Netzwerke, Sprach- und Videoanrufe.
- **Behebung von Konfigurationsfehlern in Copilot:** Identifiziert und behebt Konfigurationsfehler in Ihren Microsoft 365- und SharePoint-Umgebungen, um sichere Zugriffe durch Microsoft Copilot zu gewährleisten.
- **Verhindern von falschem Datenumgang bei Copilot Rollouts:—** Erkennt und klassifiziert alle strukturierten und unstrukturierten Daten in Hybrid- und Multi-Cloud-Umgebungen. Wendet Informationsschutz-Kennzeichnungen an, um die von unternehmenseigenen Copiloten abgerufenen Daten zu schützen.
- **Stoppen von Datenverlust durch Entdecken und Entfernen von Schatten-KI:** Erkennt die Nutzung unbefugter „Schatten-KI"-Tools und setzt Richtlinien durch, um deren Verwendung zu blockieren. Unterbindet die Nutzung und Weitergabe vertraulicher Daten durch unbefugte Tools.
- **Aufspüren und Beheben unzulässiger KI-Agenten und MCP-Verbindungen:** Verwendet ein spezielles KI-Agenten-Sicherheitstool, das auf MCP basiert und die Agentenaktivität überwacht und steuert sowie Datenrichtlinien durchsetzt.
- **Stoppen schädlicher KI-Agenten:** Verwendet ein spezielles Sicherheitstool für KI-Agenten, um Angriffe durch schädliche Agenten zu erkennen und zu blockieren.
- **Verhinderung von unzulässiger Datennutzung durch KI-Agenten:** Verwendet ein Sicherheitstool für KI-Agenten, um den Zugriff auf von KI-Agenten genutzte vertrauliche Daten zu kontrollieren und diese zu schwärzen, bevor menschliche Anwender oder andere KI-Agenten darauf zugreifen können.

©Proofpoint, Inc. 2026

So kann Proofpoint helfen

Die personen- und agentenzentrierte Proofpoint-Sicherheitsplattform nutzt die Technologien Proofpoint Nexus® sowie Proofpoint Zen™ und wird durch Proofpoint Satori™-KI-Agenten zusätzlich beschleunigt. Damit bietet Proofpoint umfassenden Schutz, der für das agentenbasierte Zeitalter entwickelt und gebaut wurde.

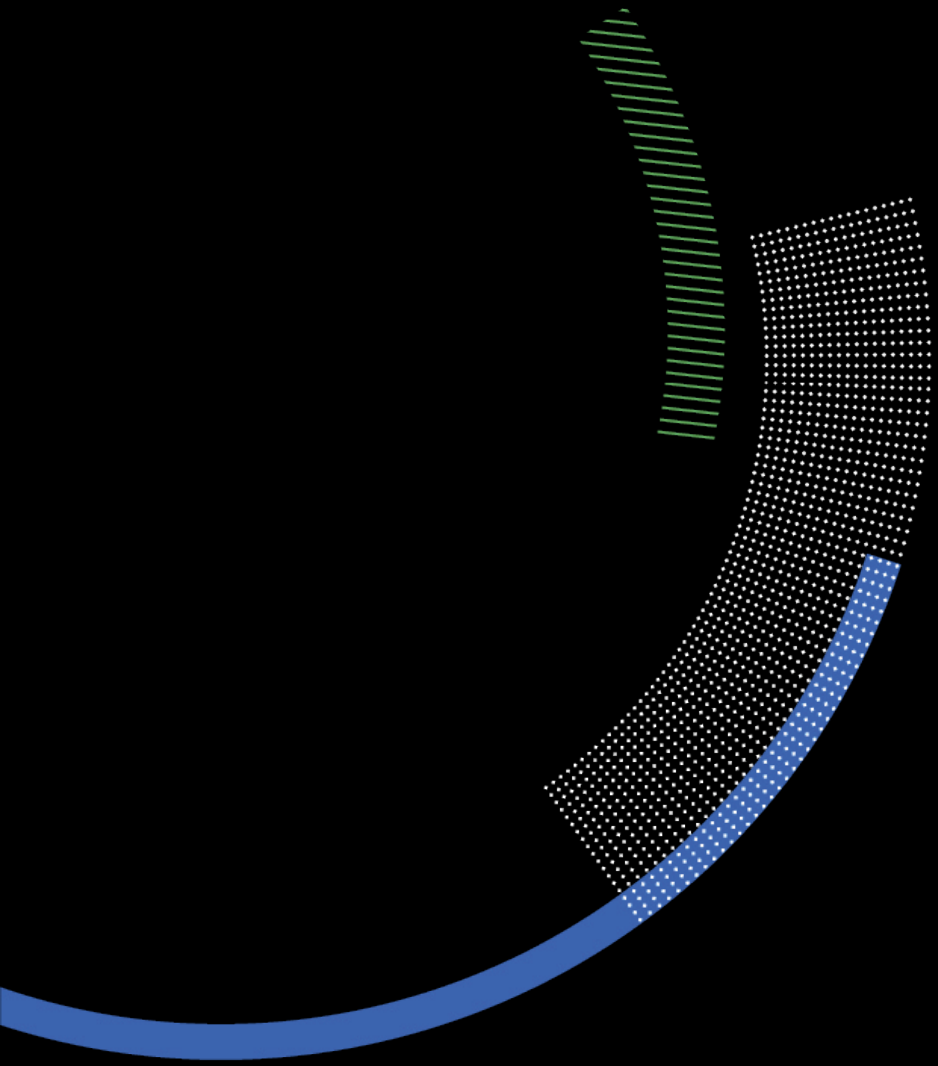
Unsere konsolidierte Lösung für sichere Zusammenarbeit behebt grundlegende Risiken am agentenbasierten Arbeitsplatz, indem sie gezielte Bedrohungen stoppt und vertrauenswürdige Interaktionen gewährleistet – zwischen menschlichen Anwendern, zwischen Agenten sowie zwischen menschlichen Anwendern und Agenten.

Gleichzeitig bietet unsere einheitliche Datensicherheitslösung vollständige Transparenz und Kontrolle über Konfigurationen, Zugriffsstatus und Exfiltrationsrisiken für alle strukturierten und unstrukturierten Daten im Unternehmen – unabhängig davon, ob diese Daten von menschlichen Anwendern, KI-Assistenten oder KI-Agenten abgerufen werden.

Ihre nächsten Schritte

- Erleben Sie die Cybersecurity-Plattform von Proofpoint live: Kontaktieren Sie uns, um eine kostenlose Demo zu vereinbaren.
- Erfahren Sie mehr darüber, wie Proofpoint den agentischen Arbeitsplatz schützt – besuchen Sie eines unserer Protect Series Events.

©Proofpoint, Inc. 2026



proofpoint®

Über Proofpoint, Inc. Proofpoint, Inc. ist weltweit führend im Bereich der menschlichen und agentenzentrierten Cybersicherheit und schützt, wie Menschen, Daten und KI-Agenten über E-Mail, Cloud und Kollaborationsplattformen miteinander verbunden sind. Proofpoint genießt das Vertrauen von mehr als 80 Unternehmen der Fortune 100, über 10.000 Großunternehmen und Millionen kleinerer Organisationen, wenn es darum geht, Bedrohungen zu stoppen, Datenverluste zu verhindern und die Widerstandsfähigkeit von Menschen und KI-Workflows zu stärken. Die Plattform für Zusammenarbeit und Datensicherheit von Proofpoint unterstützt Organisationen jeder Größe dabei, ihre Mitarbeitenden zu schützen und zu stärken, während sie KI sicher und mit Zuversicht nutzen.

Weitere Informationen unter www.proofpoint.com.

Vernetzen Sie sich mit Proofpoint: LinkedIn

Proofpoint ist eine eingetragene Marke bzw. ein Handelsname von Proofpoint, Inc. in den USA und/oder anderen Ländern. Alle weiteren Marken in diesem Text sind Eigentum ihrer jeweiligen Inhaber.

©Proofpoint, Inc. 2026