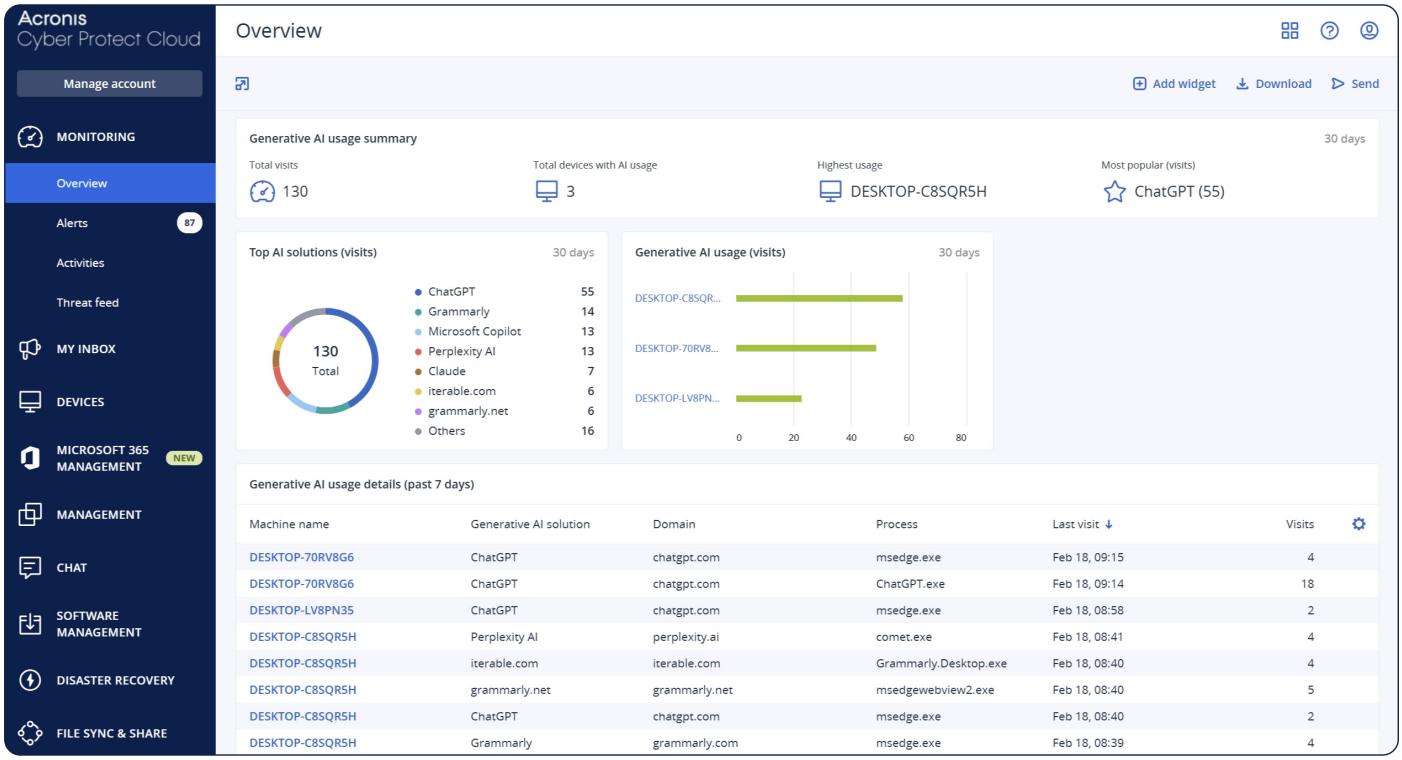
Acronis GenAI Protection

Profitieren Sie von GenAI: Erweitern Sie Ihr Portfolio und positionieren Sie sich als vertrauenswürdiger Partner für die KI-Transformation Ihrer Kunden



Generative KI verbreitet sich in KMUs rasant – oft über nicht genehmigte Privatanwender-Tools, die von der IT-Abteilung nicht überwacht werden. Zwar steigert GenAI die Produktivität, sie birgt jedoch auch neue Risiken in Bezug auf Datenschutzverletzungen, Compliance-Verstöße und Angriffsflächen. Unternehmen erwarten von ihren Service Providern, dass diese Risiken gemindert werden.

Acronis GenAI Protection ist nativ in die Acronis Plattform integriert und bietet MSPs jeder Größe eine praktische und skalierbare Möglichkeit, die Nutzung von GenAI-Tools in Kundenumgebungen zu kontrollieren und zu schützen. Dafür sind keine weiteren eigenständigen Produkte, Konsolen oder ein höherer Betriebsaufwand erforderlich.

Vollständige Transparenz über die Nutzung von GenAI-Tools

Die Lösung zeigt, welche GenAI-Tools von wem und wie oft in den Kundenumgebungen genutzt werden. Sie identifiziert Schatten-KIs, erfasst Nutzungstrends und erkennt ungewöhnliches oder riskantes Verhalten, bevor es zu Vorfällen oder Compliance-Problemen kommt.

Das Ergebnis: Die Einführung von KI wird aktiv gesteuert und überwacht. Es wird nicht erst reagiert, nachdem bereits Daten offengelegt wurden.

Verhinderung der Offenlegung sensibler Daten

GenAI-Prompts werden auf regulierte und sensible Daten wie personenbezogene Daten, geschützte Gesundheitsdaten, Zahlungskartendaten, Anmeldedaten und vertrauliche Informationen überprüft. Nicht autorisierte Übermittlungen an öffentliche oder nicht genehmigte KI-Tools werden blockiert, um Datenschutzverletzungen und regulatorische Risiken zu reduzieren.

Das Ergebnis: Kundendaten werden geschützt und Compliance-Risiken reduziert, ohne die Produktivität zu beeinträchtigen.

Verhinderung von KI-Missbrauch und schädlichen Prompts

Erkennt und blockiert bösartige oder gegen Richtlinien verstoßende Prompts, einschließlich Prompt Injection-Versuchen und anderer Techniken, die darauf abzielen, das Verhalten der KI zu manipulieren oder Kontrollmechanismen zu umgehen.

Das Ergebnis: KI-bedingte Angriffsflächen werden reduziert, während Workflows und die Integrität der KI-Outputs geschützt werden.

Wie Acronis GenAI Protection funktioniert

Zentrales Cloud-Management. Endpunktbasierter Schutz. Erkennung und Reporting in Echtzeit.

Alle wichtigen Funktionen und speziell für MSPs entwickelt

Überwachung von Schatten-KI und Reporting

Überwachen Sie die Nutzung von GenAI-Tools in Kundenumgebungen. Dabei wird erfasst, auf welche Tools von wem und wie oft zugegriffen wird. Nutzen Sie die Erkenntnisse aus Berichten und Dashboards, um Schatten-KI aufzudecken, Anomalien zu erkennen und fundierte Entscheidungen über Richtlinien zu ermöglichen.

Klassifizierung sensibler Daten

Überprüfen Sie Prompts auf regulierte und sensible Unternehmensdaten. Dazu zählen personenbezogene Daten, geschützte Gesundheitsdaten, Kartenzahlungsdaten und Daten, die als „vertraulich" gekennzeichnet sind. So behalten Sie die Kontrolle darüber, welche Daten Benutzende an externe KI-Tools weitergeben dürfen.

Schutz vor Datenverlust bei Interaktionen mit GenAI-Tools

Implementieren Sie Maßnahmen, um Datenverlust bei der Nutzung von GenAI-Tools zu verhindern. Zu diesem Zweck wird die Weitergabe sensibler Inhalte an öffentliche oder nicht genehmigte KI-Tools erkannt und unterbunden.

Erkennung schädlicher Prompts

Identifizieren Sie schädliche Prompts und Prompt Injection-Versuche, die darauf abzielen, das Verhalten der KI zu manipulieren, unsichere Inhalte einzuschleusen oder Richtlinienkontrollen zu umgehen.

„Nur erkennen"-Modus

Führen Sie das System im reinen Überwachungsmodus aus. So können Sie das KI-Nutzungsverhalten beobachten, Verstöße gegen Richtlinien aufdecken und Verhaltens-Baselines erstellen, bevor Sie die Durchsetzung aktivieren.

„Blockieren"-Modus

Aktivieren Sie den Durchsetzungsmodus, um regelwidrige oder böswillige KI-Interaktionen automatisch zu unterbinden und einen einheitlichen Schutz in allen Umgebungen durchzusetzen.

Zentrales Ereignisprotokoll

Überprüfen Sie GenAI-bezogene Erkennungen, Verstöße und Maßnahmen in einem zentralen Ereignisprotokoll, um Untersuchungen, Audits und Richtlinienanpassungen zu unterstützen.

Informative Widgets

Nutzen Sie Dashboard-Widgets, um GenAI-Aktivitäten zu verfolgen und Nutzungstrends zu analysieren. Dies ermöglicht es Ihnen, fundierte Entscheidungen über Richtlinien und deren Durchsetzung zu treffen.

Warum Acronis?

Im Gegensatz zu KI-Sicherheitstools für den Enterprise-Markt, die mit höheren Kosten, größerer Komplexität und separaten Konsolen einhergehen, wurde Acronis GenAI Protection speziell für MSPs entwickelt. Es ist Teil einer einheitlichen, mandantenfähigen Plattform. Acronis GenAI Protection bietet MSPs eine unkomplizierte Lösung, um die KI-Nutzung zu überwachen, Risiken zu minimieren und ihr Sicherheitsangebot zu erweitern, ohne dass sie weitere Einzeltools hinzufügen müssen.

Verwandeln Sie GenAI-Risiken in eine Geschäftschance für Managed Services

Wie Acronis GenAI Protection Ihr MSP-Geschäft voranbringt:

- Sie können auf eine schnell wachsende Kundennachfrage reagieren.
- Sie können Ihr Sicherheitsangebot von dem der Konkurrenz differenzieren.
- Sie können die sichere Einführung von GenAI-Tools ermöglichen, statt sie nur zu blockieren.
- Sie können Ihren Umsatz steigern, ohne den Betriebsaufwand zu erhöhen.

Persönliche Demo anfordern

Acronis

Erfahren Sie mehr auf
acronis.com