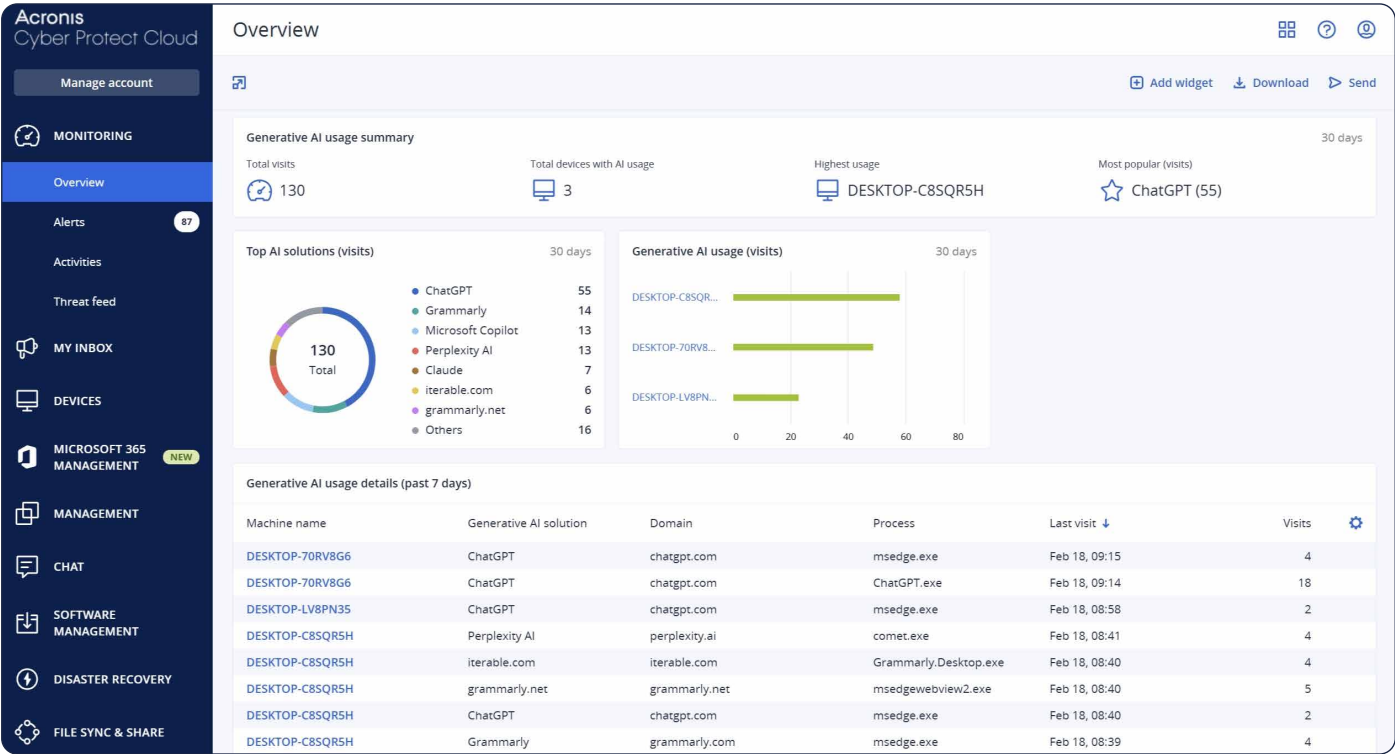


Acronis GenAI Protection

Sécurisez l'ère de la GenAI : développez vos services et positionnez-vous comme un conseiller de confiance dans le cadre de la transformation IA de vos clients.



L'IA générative se propage rapidement dans les PME, souvent via des outils grand public non autorisés, hors du contrôle des équipes IT. Si la GenAI améliore la productivité, elle crée aussi de nouveaux risques de fuite de données, de non-conformité et des surfaces d'attaque que les fournisseurs de services doivent sécuriser.

Acronis GenAI Protection, nativement intégré à la plateforme Acronis, offre aux MSP de toute taille un moyen pratique et évolutif de gouverner et sécuriser l'usage de la GenAI dans les environnements des clients, sans devoir ajouter de solution autonome, de console supplémentaire ni de charge opérationnelle.

Obtenez une visibilité complète sur l'utilisation de la GenAI

Découvrez quels outils GenAI sont utilisés dans les environnements des clients, par qui et à quelle fréquence. Identifiez l'IA fantôme, comprenez les tendances d'adoption et détectez au plus tôt les comportements anormaux ou à risque, avant qu'ils ne se transforment en incidents ou en problèmes de conformité.

Résultat : gouvernez l'adoption de l'IA en toute confiance au lieu de réagir après une fuite de données.

Empêchez l'exposition des données sensibles

Inspectez les prompts GenAI afin de détecter des données réglementées et sensibles telles que les données personnelles, de santé, les données PCI, les identifiants et des informations confidentielles. Bloquez les envois non autorisés vers des outils d'IA publics ou non autorisés afin de réduire les fuites de données et les risques réglementaires.

Résultat : protégez les données des clients et réduisez les risques de non-conformité sans freiner la productivité.

Neutralisez les prompts malveillants et les utilisations abusives de l'IA

Détectez et bloquez les prompts malveillants ou contraires à la stratégie, y compris les tentatives d'injection de prompt et autres techniques conçues pour manipuler le comportement de l'IA ou contourner les contrôles.

Résultat : limitez l'exposition aux attaques optimisées par l'IA tout en protégeant les workflows et l'intégrité des résultats.

Fonctionnement d'Acronis GenAI Protection

Gestion centralisée dans le cloud. Protection basée sur les terminaux. Détection et reporting en temps réel.

1

Gestion centralisée dans Acronis Cyber Protect Cloud

Acronis Cyber Protect Cloud



Stratégies
Activez GenAI Protection



Mode
Détection uniquement ou Bloc



Console centrale
Gérez tous les services de cyberprotection

2

Protection des terminaux et détection des risques



Agent Acronis unifié

GenAI Protection
Outils GenAI :



Surveillance de l'utilisation
Découvrez l'activité GenAI sur chaque terminal



Détection des risques
Fuite de données sensibles + prompts malveillants



Blocage/autorisation en temps réel
Selon le mode Détection uniquement ou Bloc défini dans les stratégies

3

Visibilité, journalisation et reporting

Disponible dans Acronis Cyber Protect Cloud



Journal des événements
Enregistrez toutes les détections et actions



Widgets du tableau de bord
Gagnez en visibilité sur les tendances et les risques de l'IA générative



Reporting client
Partagez facilement des informations et des rapports

Toutes les fonctionnalités dont vous avez besoin, conçues pour les MSP



Surveillance et reporting de l'IA fantôme

Surveillez l'utilisation des outils GenAI dans les environnements client, notamment les outils employés, par qui et à quelle fréquence. Exploitez le reporting et les analyses du tableau de bord pour dévoiler l'utilisation de l'IA fantôme, détecter les anomalies et appuyer les décisions stratégiques.



Classification des données sensibles

Inspectez les prompts afin de détecter les contenus réglementés et sensibles pour l'entreprise, y compris les données de type PII, PHI, liées à la norme PCI-DSS et les données identifiées comme « Confidentielles ». Renforcez le contrôle de ce que les utilisateurs peuvent partager avec des services d'IA externes.



Prévention des pertes de données (DLP) pour les interactions GenAI

Appliquez des contrôles de prévention des pertes de données dans le cadre des interactions GenAI en détectant et en bloquant les envois non autorisés de contenu sensible vers des outils d'IA publics ou non approuvés.



Détection des prompts malveillants

Identifiez les prompts malveillants et les tentatives d'injection conçues pour manipuler le comportement de l'IA, introduire du contenu dangereux ou contourner les contrôles de stratégie.



Mode détection uniquement

Exécutez en mode alerte uniquement pour observer l'utilisation de l'IA, faire remonter les violations de stratégie et établir des bases comportementales avant d'activer l'application.



Mode blocage

Activez le mode d'application pour bloquer automatiquement les interactions IA malveillantes ou non conformes à la stratégie et appliquer la protection en toute cohérence à l'ensemble des environnements.



Journal centralisé des événements

Consultez les détections, violations et actions liées à la GenAI dans un journal centralisé des événements afin de faciliter l'investigation, l'audit et l'ajustement de la stratégie.



Widgets riches en informations

Utilisez les widgets du tableau de bord pour suivre les activités de GenAI, comprendre les tendances d'utilisation et prendre des décisions de stratégie et d'application plus éclairées.



Pourquoi choisir Acronis ?

Contrairement aux outils de sécurité de l'IA pensés pour l'entreprise qui induisent des coûts, de la complexité et l'ajout de consoles distinctes, Acronis GenAI Protection est conçu pour les MSP et intégré à une plateforme multitenant unifiée. Pour les fournisseurs de services, c'est un moyen pratique de surveiller l'utilisation de l'IA, de réduire les risques et d'enrichir les offres de sécurité sans multiplier les outils.

Transformez le risque lié à la GenAI en opportunité de services managés

Avec Acronis GenAI Protection, vous pouvez :

- Répondre aux préoccupations croissantes des clients
- Permettre une adoption sûre de la GenAI au lieu de bloquer son utilisation
- Différencier vos offres de services
- Augmenter votre chiffre d'affaires sans alourdir la charge opérationnelle

Demander une démo

