

Acronis Data Loss Prevention (DLP)

für Acronis Cyber Protect Cloud

Schützen Sie die sensiblen Daten Ihrer Kunden schnell und mit minimalem Aufwand

Seit Jahren gelingt es Unternehmen kaum, sensible Daten vor nicht autorisierten Zugriffen und Exfiltration zu schützen – Gefahren, die durch externe Angriffe oder Insider-Bedrohungen (z. B. IT-Konfigurationsfehler, menschliche Fehler oder böswilliges Verhalten) entstehen. Die Folge sind häufig peinliche Schlagzeilen, verlorenes Vertrauen bei Kunden und Partnern, finanzielle Verluste, Personalprobleme und behördliche Sanktionen.

Die größten Hürden für die Einführung wichtiger DLP-Funktionen sind deren Komplexität, die hohen Bereitstellungskosten sowie der lange Zeitraum bis zur Amortisierung, da DLP-Richtlinien nicht universell sind,

sondern für jedes Unternehmen maßgeschneidert werden müssen. Aus diesen Gründen wurde DLP bisher nur bei sehr großen Unternehmen implementiert.

Acronis DLP bietet Ihnen unvergleichliche Einfachheit bei Bereitstellung, Konfiguration und Verwaltung, um Datenlecks aus Client-Workloads zu verhindern und die Einhaltung gesetzlicher Vorschriften zu stärken. Mit einer einzigartigen verhaltensbasierten Technologie werden automatisch kundenspezifische Richtlinien erstellt und kontinuierlich gepflegt, ohne dass Monate für die Bereitstellung vergehen, ganze Teams für die Pflege benötigt werden oder ein Dokortitel in Datenschutzrecht benötigt wird, um die Problematik zu verstehen.

Verbessern Sie Ihr Service-Paket mit optimierten DLP-Funktionen

Inhaltsbezogene DLP-Kontrollen für mehr als 70 Kanäle	Automatische Erstellung und Erweiterung verhaltensbasierter DLP-Richtlinien	Sofortige Reaktion bei DLP-Ereignissen
Schützen Sie die vertraulichen Daten Ihrer Kunden und verhindern Sie, dass Daten von Kunden-Workloads über Peripheriegeräte und Netzwerkverbindungen kompromittiert werden, indem Sie den Inhalt und Kontext von Datenübertragungen analysieren und richtlinienbasierte präventive Kontrollen durchsetzen.	Es ist nicht notwendig, die Details des Kundenunternehmens aufzuschlüsseln und Richtlinien manuell zu definieren. Stattdessen wird automatisch ein Profil der Datenflüsse erstellt, das als Grundlage für die Erstellung und kontinuierliche Anpassung der DLP-Richtlinien an die sich ständig verändernden Geschäftsprozesse dient. Auf diese Weise wird der Schutz vor den häufigsten Ursachen für Datenlecks gewährleistet.	Ermöglichen Sie schnelle Reaktionen sowie forensische Untersuchungen und vereinfachen Sie die Pflege der DLP-Richtlinien mithilfe zentraler Überwachungsprotokolle und Echtzeitwarnungen zu Sicherheitsereignissen. Vereinfachen Sie die Berichterstellung mit informativen Widgets.

Erschließung neuer Umsatzmöglichkeiten	Minimierung des Aufwands	Minimierung von Datenverlustrisiken und Verbesserung der Compliance	Gewährleistung kundenspezifischer Richtlinien	Schnellere Reaktion bei DLP-Ereignissen
Steigern Sie Ihre Umsätze pro Kunde und gewinnen Sie weitere Kunden mit Managed Services für DLP (oder, bei VARs, mit einer DLP-Lösung), die für KMUs und Mittelständler geeignet sind.	Erweitern Sie Ihr Portfolio um einen DLP-Service, der die Verwaltung nicht komplizierter macht, die Kosten nicht erhöht und für den kein zusätzliches Personal erforderlich ist.	Erkennen und verhindern Sie das Abfließen sensibler Daten über zahlreiche lokale und Netzwerkkanäle.	Erstellen Sie ein Profil der zulässigen Datenflüsse, um zu gewährleisten, dass jeder Kunde eine maßgeschneiderte Richtlinie erhält.	Reagieren Sie schnell auf DLP-Ereignisse und nutzen Sie zuverlässige Audit-Funktionen, einschließlich richtlinienbasierter Warnmeldungen und einem zentralen Überwachungsprotokoll.

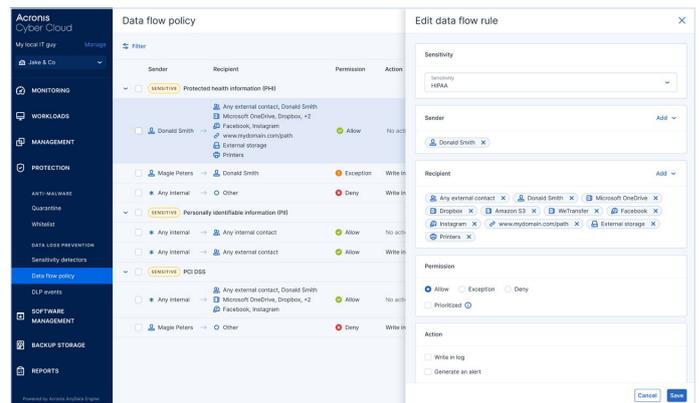
Zeitplan: Bereitstellung Ihrer Services mit Acronis DLP

10 Minuten ●	ca. 2–6 Wochen ●	ca. 1–2 Tage ●	Automatisch ●	ca. 1–3 Stunden/ Monat/Kunde ●
Bereitstellung des Agenten für Acronis Cyber Protect Cloud	Erstellung einer DLP-Basisrichtlinie	Validierung bei Kunden	Automatische Erweiterung der Richtlinie	Reporting und Optimierung

Funktionsweise von Acronis DLP

Umfassender Schutz, der die Anforderungen der Kunden erfüllt und dabei unglaublich einfach ist:

- Schützt sensible Daten, die über verschiedenste Kommunikationskanäle zwischen Benutzer:innen und Systemen übertragen werden, darunter Netzwerkverbindungen (z. B. Sofortnachrichten) sowie Peripheriegeräte (z. B. USB-Laufwerke).
- Bietet sofort einsatzbereite Datenklassifizierungen für gängige Vorschriften wie DSGVO, HIPAA und PCI-DSS.
- Um Richtlinien automatisch erstellen, empfehlen und anpassen zu können, werden Profile für ausgehende Datenflüsse von Workloads erstellt. Dadurch ist der Schutz vor den häufigsten Ursachen für nicht autorisierte Datenübertragungen an Dritte gewährleistet.
- Bietet kontinuierliche Überwachung auf DLP-Vorfälle, einschließlich mehrerer Optionen zur Richtliniendurchsetzung.
- Ermöglicht die automatische und kontinuierliche Anpassung der Richtlinien an Geschäftsprozesse.
- Unterstützt dank zuverlässiger Audit- und Protokollierungsfunktionen schnelle Reaktionen und forensische Untersuchungen nach erfolgreichen Kompromittierungen.
- Verwendet die zentrale Acronis Cyber Protect Cloud Konsole sowie den bereits vorhandenen Agenten für Transparenz und Klassifizierung von Daten.



Kontrollierte Kanäle

- Wechselmedien
- Drucker
- Umgeleitete zugeordnete Laufwerke
- Umgeleitete Zwischenablagen
- Alle SMTP-E-Mails, Microsoft Outlook (MAPI), IBM Notes (NRPC)
- 7 Instant Messenger
- 16 Webmail-Dienste
- 28 Dateifreigabedienste
- 12 soziale Netzwerke
- Lokale Dateifreigaben, Webzugriff und FTP-Dateiübertragungen

Kernfunktionen

- Anpassbare DLP-Regeln
- Kontext- und inhaltsbezogene DLP-Kontrollen
- Automatische Erstellung und Erweiterung von DLP-Richtlinien
- Vorkonfigurierte Datenklassifizierungen für personenbezogene Daten, Gesundheitsdaten, Zahlungskartendaten und als vertraulich gekennzeichnete Daten
- Strikte sowie adaptive Durchsetzung von DLP-Richtlinien
- Unterstützung für Blockierungs-Ausnahmen
- Webbrowser-unabhängige Kontrollen für Datenübertragungen
- Optische Zeichenerkennung (OCR) im Agenten
- Echtzeitwarnungen
- Richtlinienbasierte Protokollierungen und Warnmeldungen
- Zentrales Cloud-natives Überwachungsprotokoll
- DLP-Protokoll-Ereignisanzeige mit einfachen Filterungs- und Suchfunktionen
- Informative Berichte
- Bildschirmmeldungen an die Endnutzer