
# Advanced Data Loss Prevention (DLP)

## für **Acronis** Cyber Protect Cloud

### Voraussichtlich erhältlich im März 2022

### Eine DLP-Lösung für MSPs mit automatischer Erstellung kundenspezifischer Richtlinien

Da 72 % der Mitarbeiter vertrauliche Unternehmensdaten weitergeben, überrascht es nicht, dass dem Ponemon Institute zufolge 45 % aller Kompromittierungen durch Insider verursacht werden. Traditionelle DLP-Lösungen zur Verringerung dieser Risiken erfordern jedoch fundierte und teure Sicherheitskompetenz. DLP-Richtlinien sind immer unternehmensspezifisch und hängen von den individuellen Kundenanforderungen ab. Sie müssen diese Anforderungen ermitteln und dann die DLP-Richtlinien manuell und aufwändig daran anpassen.

Mit Acronis Advanced DLP erhalten Sie unübertroffen einfache Provisioning-und Management-Funktionen, damit Sie Datenverlust von Kunden-Workloads über Peripheriegeräte und Netzwerkverbindungen verhindern können. Dank der automatisch generierten DLP-Basisrichtlinien können Sie für jeden Kunden unternehmensspezifische Richtlinien zuverlässig und effizient erstellen.

### Verbessern Sie Ihr Service-Paket mit optimierten DLP-Funktionen

| KONTEXT- UND INHALTSBEZOGENE DLP-KONTROLLEN | AUTOMATISCHE GENERIERUNG KUNDENSPEZIFISCHER DLP-BASISRICHTLINIEN | ADAPTIVE DURCHSETZUNG VON DLP-RICHTLINIEN |
|---|---|---|
| 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. | Die Erfassung der Unternehmensanforderungen und die Erstellung unternehmensspezifischer DLP-Basisrichtlinien erfolgen jetzt automatisch basierend auf überwachten ausgehenden vertraulichen Datenflüssen. Kunden können die Richtlinien überprüfen, bevor sie vom System durchgesetzt werden. | Die manuelle Verwaltung und Anpassung von DLP-Richtlinien nach der ersten Durchsetzung ist nicht mehr notwendig. Dank einer Option für die adaptive Richtliniendurchsetzung lassen sich Richtlinien automatisch für neue, in Kunden-Workloads vorher ungenutzte Datenflüsse erweitern. |

### Neue Rentabilitätschancen

- **Verbessern Sie Ihren Umsatz pro Kunde** mit stark nachgefragten MSP-verwalteten DLP-Services.
- **Gewinnen Sie mehr Kunden** mit einem Beobachtungsmodus, der den Mehrwert Ihres Service und die Bedeutung von DLP verdeutlicht.
- **Senken Sie Ihre Kosten und erhöhen Sie Ihre Margen** durch einfaches Service-Tiering mit einer integrierten Plattform für Backup und Disaster Recovery, Malware-Schutz der nächsten Generation, E-Mail-Sicherheit, Workload-Verwaltung und DLP.

### Mehr Produktivität und weniger Kosten

- **Verringern Sie den Zeitaufwand für Provisioning und Konfiguration** durch die automatisierte Erstellung kundenspezifischer DLP-Basisrichtlinien.
- **Passen Sie DLP-Richtlinien an geschäftliche Anforderungen an und reduzieren Sie Fehler.** Während der Erstellung der Basisrichtlinien können Endbenutzer die Übertragung vertraulicher Daten begründen – und Kunden können die Richtlinien vor der Durchsetzung validieren.
- **Vereinfachen Sie Compliance-Berichte und verbessern Sie den Überblick über die DLP-Performance** durch eine konfigurierbare Protokollsammlung, Warnungen und aussagekräftige Widgets.

### Weniger Datenverlustrisiken für Kunden

- **Minimieren Sie die Insider-bezogenen Datenverlustrisiken**, indem Sie die Kompromittierung vertraulicher Informationen über Peripheriegeräte und Netzwerkverbindungen verhindern.
- **Minimieren Sie die Folgen menschlicher Fehler und erzwingen Sie unternehmensweit geeignete Datennutzungsrichtlinien.**
- **Verbessern Sie die Compliance Ihrer Kunden** durch den Schutz von Daten, die Vorschriften unterliegen.

## Differenzieren Sie Ihre DLP-Services gegenüber Ihren Mitbewerbern

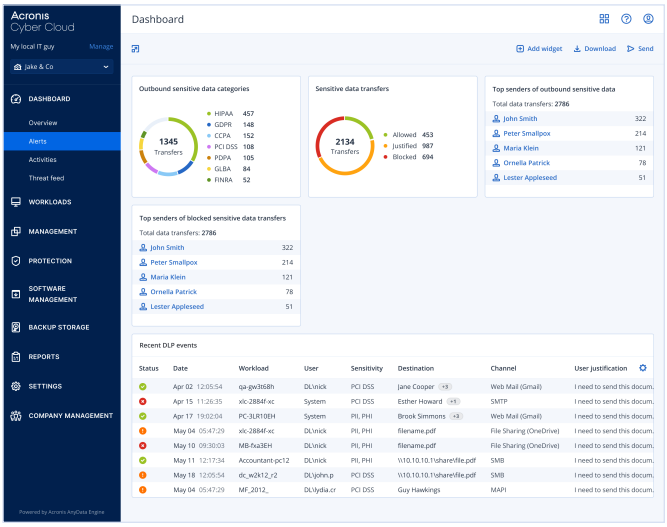
| AUTOMATISIERTE ERSTELLUNG VON DLP-RICHTLINIEN | KUNDENSPEZIFISCHE DLP-RICHTLINIEN | UNÜBERTROFFENE ANZAHL ÜBERWACHTER KANÄLE | UMFASSENDE DLP-KONTROLLEN | ZENTRALE CYBER PROTECTION ÜBER NUR EINE KONSOLE |
|---|---|---|---|---|
| Verringern Sie die Zahl manueller Schritte und das Risiko für Fehler. Vereinfachen Sie das Provisioning, indem die DLP-Basisrichtlinien für jeden Kunden automatisch generiert werden. | Überwachen Sie alle ausgehende vertraulichen Datenflüsse, damit die Geschäftsprozesse automatisch einer kundenspezifischen DLP-Richtlinie zugeordnet werden können. Beziehen Sie für mehr Genauigkeit optional Endbenutzer mit ein und bitten Sie Kunden vor der Richtliniendurchsetzung, diese zu validieren. | Kontrollieren Sie Datenflüsse aus lokalen und Netzwerkkanälen, einschließlich Wechselmedien, Druckern, umgeleiteten zugeordneten Laufwerken und Zwischenablagen, E-Mails und Webmails, Instant Messengern, Dateifreigabediensten, sozialen Netzwerken sowie Netzwerkprotokollen. | Gewährleisten Sie die Browser-unabhängige Kontrolle von Datenübertragungen zwischen sozialen Medien, Webmails und Dateifreigabediensten. Untersuchen Sie die Inhalte ausgehender Sofortnachrichten und erkennen Sie vertrauliche Daten in Bildern auf Remote- und Offline-Rechnern. | Senken Sie Gesamtbetriebskosten und Verwaltungsaufwand und erhöhen Sie Ihre Margen mit einer zentralen Lösung, die Backup und Disaster Recovery, Malware-Schutz der nächsten Generation, E-Mail-Sicherheit, Workload-Verwaltung sowie DLP integriert. |

## Vereinfachte Prozesse für Provisioning sowie Erstellung und Verwaltung von DLP-Richtlinien

Zur Optimierung der Provisioning- und Verwaltungsprozesse bei MSPs bietet Advanced Data Loss Prevention (DLP) zwei Modi:

### Beobachtungsmodus

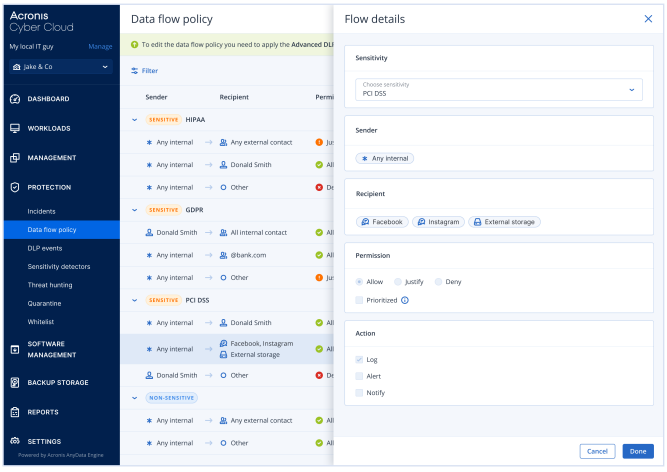
Demonstrieren Sie den Mehrwert Ihrer DLP-Services und machen Sie die Bedeutung von DLP deutlich. Im Beobachtungsmodus überwacht der Agent die Endpunkte von Kunden auf ausgehende vertrauliche Datenflüsse. Dabei werden entweder automatisch DLP-Basisrichtlinien generiert oder es werden Begründungen der Endbenutzer für die riskantesten Datenübertragungen herangezogen.




### Durchsetzungsmodus

Sobald eine DLP-Richtlinie vom Kunden validiert wurde, können Sie diese durchsetzen und die Kundendaten schützen. Im Durchsetzungsmodus können Sie wählen, wie DLP-Richtlinien durchgesetzt werden sollen:

- **Strikte Durchsetzung:** DLP-Richtlinien werden gemäß Definition durchgesetzt, ohne sie mit neuen Datenflussregeln zu erweitern. Datenübertragungen, die nicht der definierten Datenflussregel entsprechen, werden blockiert, es sei denn der Endbenutzer beantragt eine einmalige geschäftsbezogene Ausnahme, um die Blockierung aufzuheben.
- **Adaptive Durchsetzung:** DLP-Richtlinien werden durchgesetzt, können aber mit neuen Regeln für zuvor nicht beobachtete geschäftsbezogene Datenflüsse erweitert werden.




Acronis

Weitere Informationen unter
www.acronis.com