iloogi

Advanced Data Loss Prevention (DLP)

For **Acronis** Cyber Protect Cloud

Protect clients' sensitive data with the ease and speed you need

For years, organizations have had little success protecting sensitive data from unauthorized access and exfiltration via external attacks or insider risks such as IT misconfigurations, human error or threats. This has left them exposed to consequences like embarrassing headlines, damaged customer and partner trust, equity losses, HR problems and regulatory sanctions.

Unfortunately, the key DLP adoption obstacles of complexity, deployment costs, and a long time to value due to DLP policies being not-universal but highly business-specific, have remained insurmountable for most companies other than the very largest enterprises.

Acronis Advanced DLP empowers you with unmatched provisioning, configuration, and management simplicity, to prevent data leakage from client workloads and strengthen regulatory compliance. A unique behavior-based technology automatically creates and continuously maintains business-specific policies, without requiring months to deploy, teams to maintain or a Ph.D. in privacy law to understand.

Enhance your service stack with streamlined data loss prevention

Content-aware DLP controls across 70+ channels	Automatic, behavior-based DLP policy creation and extension	Prompt reactiveness to DLP events
Protect clients' sensitive data by preventing data leakage from workloads via peripheral devices and network communications; by analyzing the content and context of data transfers; and by enforcing policy-based preventive controls.	No need to drill down into client business details and define policies manually. Automatically profile sensitive data flows to create and continuously adjust DLP policies to ever-changing business specifics, ensuring protection against the most common causes of data leaks.	Enable rapid response and forensic investigations and simplify DLP policy maintenance via centralized audit logs and real-time alerts of security events. Ease reporting with information-rich widgets.

Unlock new profitability opportunities	Minimize efforts to value	Mitigate data leak risks and strengthen compliance	Ensure client-specific policies	Enable better reactiveness to DLP events
Improve your revenue per client and attract more clients with managed DLP services (or a DLP solution — for VARs) accessible to SMBs and mid-market clients.	Expand your portfolio with a DLP service that doesn't increase your management complexity, costs, and headcount to streamline your efforts.	Detect and prevent sensitive information leakage across a vast array of local and network channels.	Profile sensitive data flows to ensure business-specific policies for each client.	Respond rapidly to DLP events and leverage robust auditing with policy-based alerting and logging in a centralized audit log.

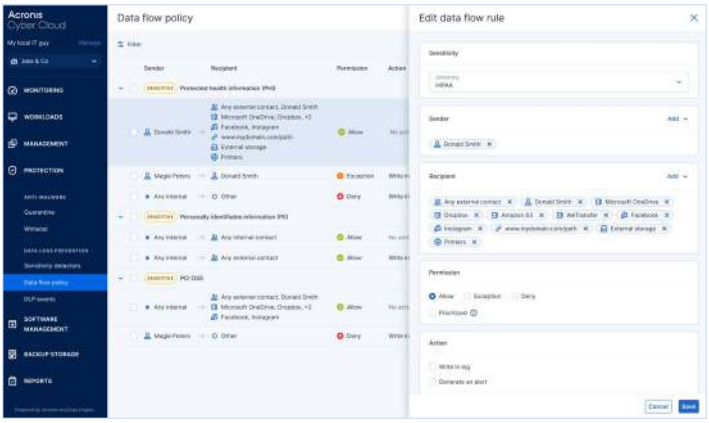
Timeline: How to provision your services with Advanced DLP

10 minutes	~ 2-6 weeks	~ 1-2 days	Automatic	~ 1-3 hours/month/client
Deploy Acronis Cyber Protect Cloud agent	**Initial DLP policy generation**	**Validation with clients**	**Automatic policy extention**	**Reporting and fine-tuning**

What Advanced DLP does

Comprehensive protection that fulfills client requirements with a never-before-seen level of simplicity:

- Protects sensitive data transferred via a wide array of user and system communications, including network communications such as instant messaging and peripheral devices like USBs.
- Offers out-of-the-box sensitive data classifiers for common regulatory frameworks including GDPR, HIPAA and PCI DSS.
- Profiles outgoing sensitive data flows from workloads to automatically create, recommend and enable tuning of policies — ensuring protection against the most common causes of data transfers to unauthorized parties.
- Provides continuous monitoring for DLP incidents with multiple policy enforcement options.
- Enables ongoing automated policy adjustments to business specifics.
- Enables rapid response and post-breach forensic investigations with robust audit and logging capabilities.
- Uses the unified Acronis Cyber Protect Cloud console and agent for data visibility and classification.



Controlled channel

- Removable storage
- Printers
- Redirected mapped drives
- Redirected clipboards
- Any SMTP emails, Microsoft Outlook (MAPI), IBM Notes (NRPC)
- 7 Instant messengers
- 16 webmail services
- 28 file sharing services
- 12 social networks
- Local file shares, web access, and FTP file transfers

Key features

- Context- and content-aware DLP controls
- Automatic DLP policy creation and extension
- Pre-built data classifiers for PII, PHI, PCI DSS, “Marked as Confidential”
- Strict and adaptive DLP policy enforcement
- Policy block override support if exceptions are needed
- Web browser-independent control of data transfers
- Agent-resident optical character recognition (OCR)
- Real-time alerting
- Policy-based logging and alerting
- Centralized cloud-native audit log
- DLP log event viewer with easy filtering and search capabilities
- Information-reach reporting
- On-screen notifications to end users

Acronis

Learn more at
www.acronis.com