Advanced Data Loss Prevention (DLP)

For **Acronis** Cyber Protect Cloud

Early access program

Leverage a DLP solution designed for MSPs with automatic, client-specific policy creation

Given that 72% of employees share sensitive company information, it's no surprise that the Ponemon Institute found that insider-related incidents account for 45% of all breaches. Yet traditional DLP solutions that remediate those risks require extensive and costly security expertise to provision and operate – DLP policies are not universal but business-specific, turning configuration into a long, manual and costly process of learning a client's unique business needs and mapping those manually to DLP policies.

Acronis Advanced DLP empowers you with unmatched provisioning and management simplicity, to prevent data leakage from clients' workloads via peripheral devices and network communications. With automatic, baseline DLP policy generation, you can accurately and efficiently create business-specific policies for each client.

Enhance your service stack with streamlined data loss prevention

CONTEXT- AND CONTENT-AWARE DLP CONTROLS	AUTOMATIC CLIENT-SPECIFIC BASELINE DLP POLICY GENERATION	ADAPTIVE DLP POLICY ENFORCEMENT
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 enforcing policy-based preventive controls.	Stop drilling down into client business details and defining policies manually. Business-specific, baseline DLP policies are created automatically by monitoring sensitive, outgoing data flows. Clients can validate these policies before the system enforces them.	Eliminate manual work usually needed to manage and adjust a DLP policy after initial enforcement. An adaptive policy-enforcement option automatically expands the enforced policy with new, previously unused data flows detected on clients' workloads.

Unlock new profitability opportunities

- **Improve your revenue per client** with highly demanded MSP-managed DLP services
- **Attract more clients** by demonstrating your service value with an observation mode that boosts clients' DLP awareness
- **Control your TCO and enable better margins** with easier service-tiering using a single, integrated platform for backup and disaster recovery, next-generation anti-malware, email security, workload management and DLP

Improve your productivity and avoid runaway costs

- **Reduce the time spent on provisioning and configuration** via automated, client-specific, baseline DLP policy creation
- **Align DLP policies with business requirements and minimize errors** with optional end-user justification of sensitive-data transfers during baseline policy creation and easy, pre-enforcement, client validation
- **Simplify compliance reporting and increase visibility of DLP performance** through configurable log collection, alerting and informative widgets

Reduce data leakage risks for clients

- **Minimize clients' insider-related data breach risks** by preventing sensitive information leakage via peripheral devices and network communications
- **Minimize the impact of human errors and enforce acceptable** data use policies company-wide
- **Strengthen clients' regulatory compliance** by protecting data that is subject to regulations

Differentiate your DLP services with an edge over the competition

AUTOMATED DLP POLICY GENERATION	CLIENT-SPECIFIC DLP POLICIES	UNMATCHED ARRAY OF CONTROLLED CHANNELS	COMPREHENSIVE DLP CONTROLS	CENTRALIZED CYBER PROTECTION VIA A SINGLE CONSOLE
Minimize manual work and the risk of errors. Simplify provisioning by automatically generating a baseline DLP policy for each client.	Monitor outgoing sensitive data flows across the organization to automatically map client's business processes to a DLP policy adjusted to their specifics. Leverage optional end-user assistance for higher accuracy and request client validation before enforcing a policy.	Control data flows across local and network channels, including removable storage, printers, redirected mapped drives and clipboard, emails and webmails, instant messengers, file sharing services, social networks, and network protocols.	Ensure web-browser-independent control of data transfers to social media, webmail and file sharing services. Leverage content inspection of outgoing instant message and sensitive data detection in images on remote and offline computers.	Control your TCO, reduce management overhead and boost margins using a single solution that integrates backup, disaster recovery, next-generation anti-malware, email security, workload management and DLP.

Simplify client provisioning and DLP policy generation and management

To help MSPs streamline their provisioning and management tasks, Advanced Data Loss Prevention (DLP) works in 2 different modes:

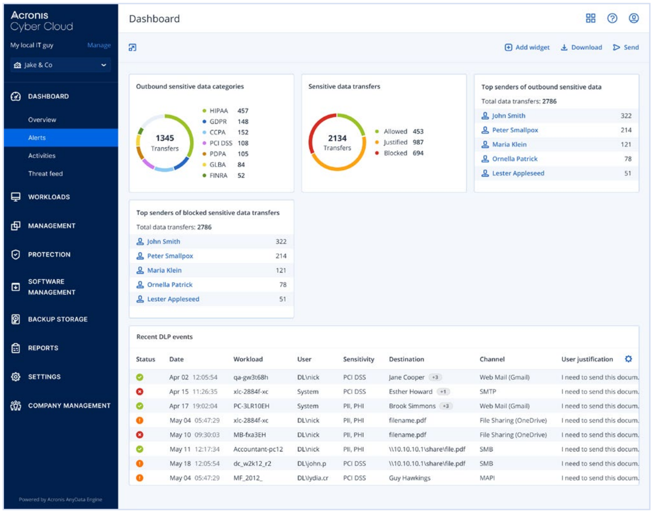
Observation mode

Effortlessly provision DLP services, removing the complexity of initial policy creation. In the observation mode, the agent monitors clients' endpoint computers for outgoing, sensitive data flows to generate the baseline DLP policy automatically or, optionally, with end-user justification of the most risky data transfers.

Enforcement mode

Once the DLP policy is validated with clients, you can enforce it to start protecting their data. Enforcement mode enables you to select how to enforce DLP policies:

- **Strict enforcement** – enforces the DLP policy as defined, without extending it with new data flow rules. Any data transfer that doesn't match a defined data flow rule in the policy is blocked unless the end-user requests a one-time business-related exception for enabling a block override.
- **Adaptive enforcement** – enforces the DLP policy but offers flexibility extending it with new rules for allowing previously unobserved business-related data flows.



Dashboard

Outbound sensitive data categories

1345 Transfers

HIPAA	457
GDPR	148
CCPA	152
PCI DSS	108
PDPA	105
GLBA	84
FINRA	52

Sensitive data transfers

2134 Transfers

Allowed	453
Justified	987
Blocked	694

Top senders of outbound sensitive data

Total data transfers: **2786**

John Smith	322
Peter Smallpox	214
Maria Klein	121
Ornella Patrick	78
Lester Appleseed	51

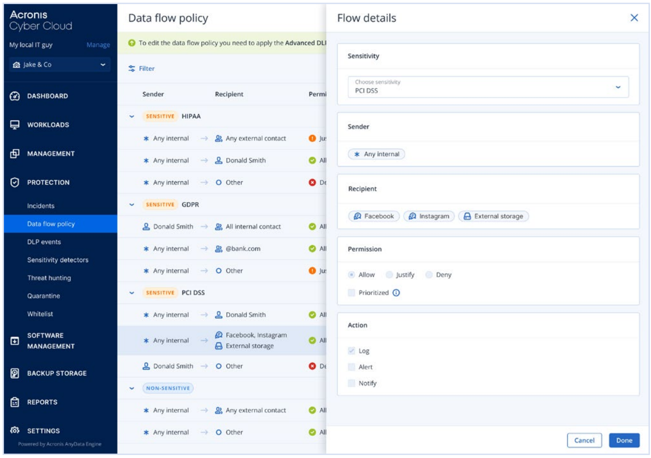
Top senders of blocked sensitive data transfers

Total data transfers: **2786**

John Smith	322
Peter Smallpox	214
Maria Klein	121
Ornella Patrick	78
Lester Appleseed	51

Recent DLP events

Status	Date	Workload	User	Sensitivity	Destination	Channel	User justification
✓	Apr 02 12:05:54	qa-gw3t68h	DL\nick	PCI DSS	Jane Cooper +3	Web Mail (Gmail)	I need to send this docum.
✕	Apr 15 11:26:35	xlc-2884f-xc	System	PCI DSS	Esther Howard +1	SMTP	I need to send this docum.
✓	Apr 17 19:02:04	PC-3LR10EH	System	PII, PHI	Brook Simmons +3	Web Mail (Gmail)	I need to send this docum.
!	May 04 05:47:29	xlc-2884f-xc	DL\nick	PII, PHI	filename.pdf	File Sharing (OneDrive)	I need to send this docum.
✕	May 10 09:30:03	MB-fxa3EH	DL\nick	PII, PHI	filename.pdf	File Sharing (OneDrive)	I need to send this docum.
✓	May 11 12:17:34	Accountant-pc12	DL\nick	PII, PHI	\\10.10.10.1\share\file.pdf	SMB	I need to send this docum.
!	May 18 12:05:54	dc_w2k12_r2	DL\john.p	PCI DSS	\\10.10.10.1\share\file.pdf	SMB	I need to send this docum.
!	May 04 05:47:29	MF_2012_	DL\lydia.cr	PCI DSS	Guy Hawkings	MAPI	I need to send this docum.



Data flow policy

To edit the data flow policy you need to apply the **Advanced DL**

	Sender	Recipient	Permi
SENSITIVE	HIPAA		
	Any internal	Any external contact	Ju
	Any internal	Donald Smith	All
	Any internal	Other	De
SENSITIVE	GDPR		
	Donald Smith	All internal contact	All
	Any internal	@bank.com	All
	Any internal	Other	Ju
SENSITIVE	PCI DSS		
	Any internal	Donald Smith	All
	Any internal	Facebook, Instagram External storage	All
	Donald Smith	Other	De
NON-SENSITIVE			
	Any internal	Any external contact	All
	Any internal	Other	All

Flow details

Sensitivity

Choose sensitivity: PCI DSS

Sender

Any internal

Recipient

Facebook Instagram External storage

Permission

● Allow ○ Justify ○ Deny

□ Prioritized

Action

☑ Log

□ Alert

□ Notify

Acronis

Learn more at
www.acronis.com