Acronis

#CyberFit

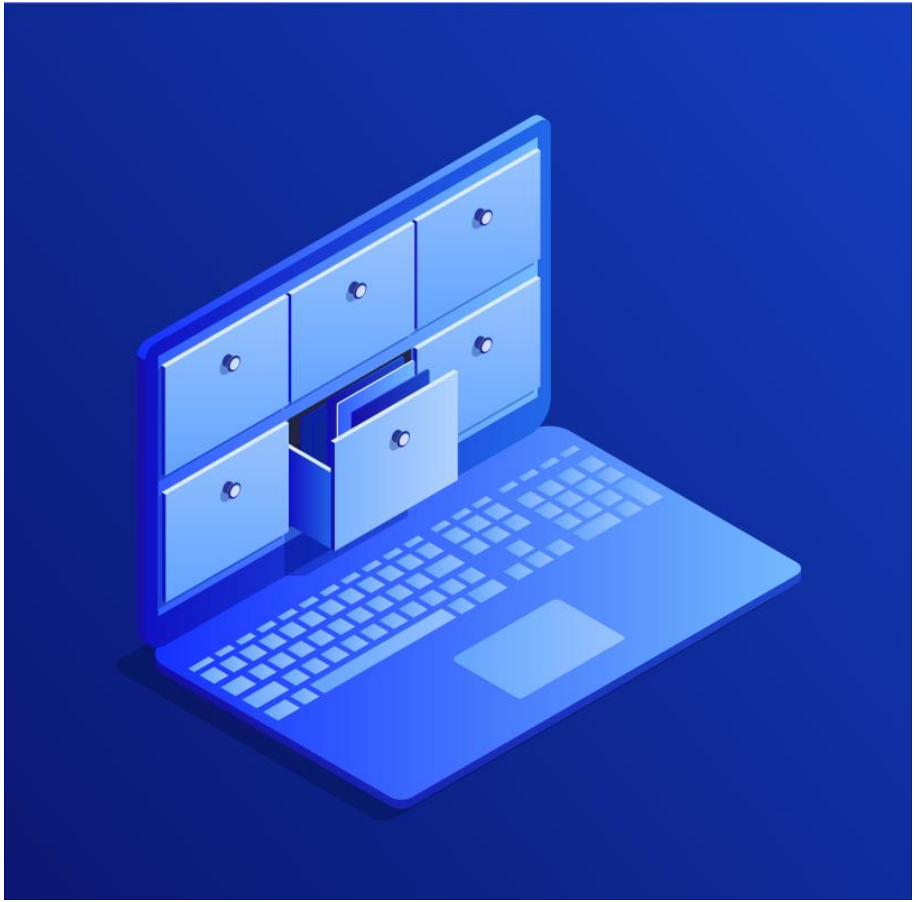
Acronis Cyber Protect Cloud with Advanced DLP*

Early access

* Data Loss Prevention

Agenda

1. What is DLP
2. DLP Essentials
3. DLP Market
4. Challenges with Current DLP Solutions
5. Advanced DLP: Value for MSPs
6. Licensing
7. How to Position your Services with Advanced DLP to Clients?
8. DLP Service Provisioning Flow
9. How to Package Services with Advanced DLP?
10. Competitive Positioning
11. Qualification Questions and Objections Handling
12. Appendix: Glossary



Acronis

#CyberFit

What is DLP?

The Data Loss Problem

What is data loss/leak?

- Breach of security in which confidential, sensitive or protected data is accidentally or deliberately released to an untrusted environment or unauthorized users outside or inside the organization

What is leaked?

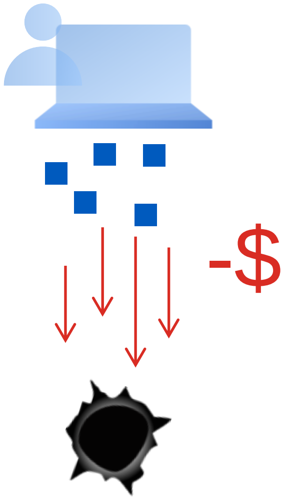
- Payment card data, client/employee personally identifiable information (PII), patient health information (PHI), intellectual property (IP), confidential information, trade secrets, state classified data…

How data gets leaked?

- External attacks: malware infiltration through software vulnerabilities, hacking, social engineering (e.g. phishing)
- Internal sources: insider mistakes, negligence, misconduct, theft; system glitches

What are the consequences?

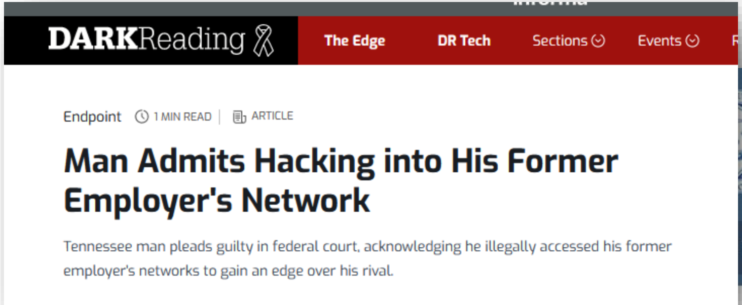
- Financial and reputational damages, loss of business
- Large fines and expensive litigations
- Damage to national security



56% Incidents relating to negligence	**26%** Incidents relating to criminal insider	**18%** Incidents relating to user credential theft
$6.6M Annualised cost for negligence	**$4.1M** Annualised cost for criminal insider	**$4.6M** Annualised cost for credential theft

Source: "Global Cost of Insider Threats", Ponemon Institute, 2022

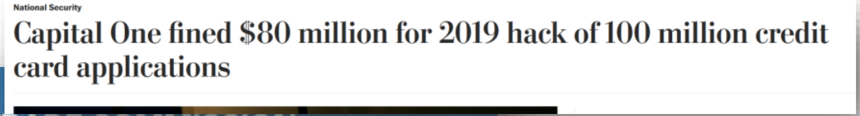
Data Theft - Breaking News



Endpoint 1 MIN READ | ARTICLE

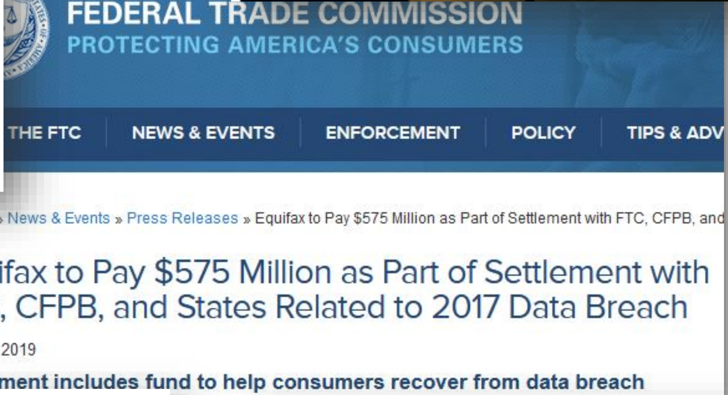
Man Admits Hacking into His Former Employer's Network

Tennessee man pleads guilty in federal court, acknowledging he illegally accessed his former employer's networks to gain an edge over his rival.



National Security

Capital One fined $80 million for 2019 hack of 100 million credit card applications

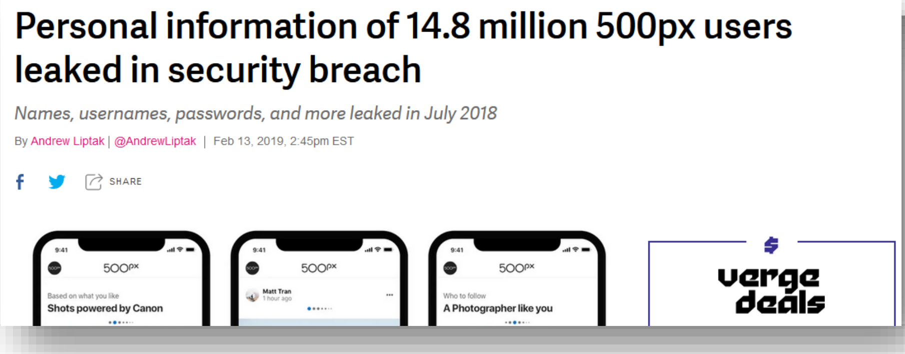


Home » News & Events » Press Releases » Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and

Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach

July 22, 2019

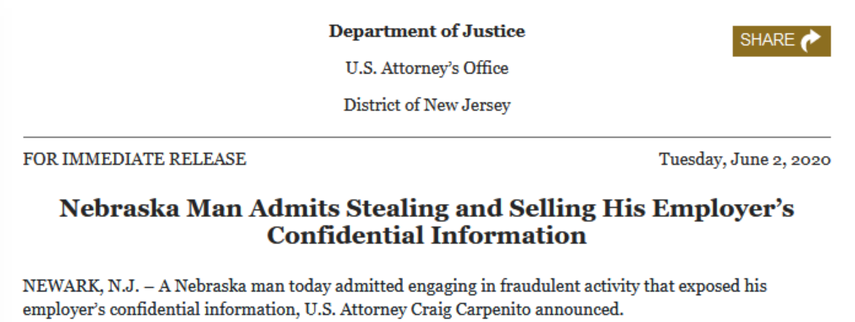
Settlement includes fund to help consumers recover from data breach



Personal information of 14.8 million 500px users leaked in security breach

Names, usernames, passwords, and more leaked in July 2018

By Andrew Liptak | @AndrewLiptak | Feb 13, 2019, 2:45pm EST



Department of Justice

U.S. Attorney's Office

District of New Jersey

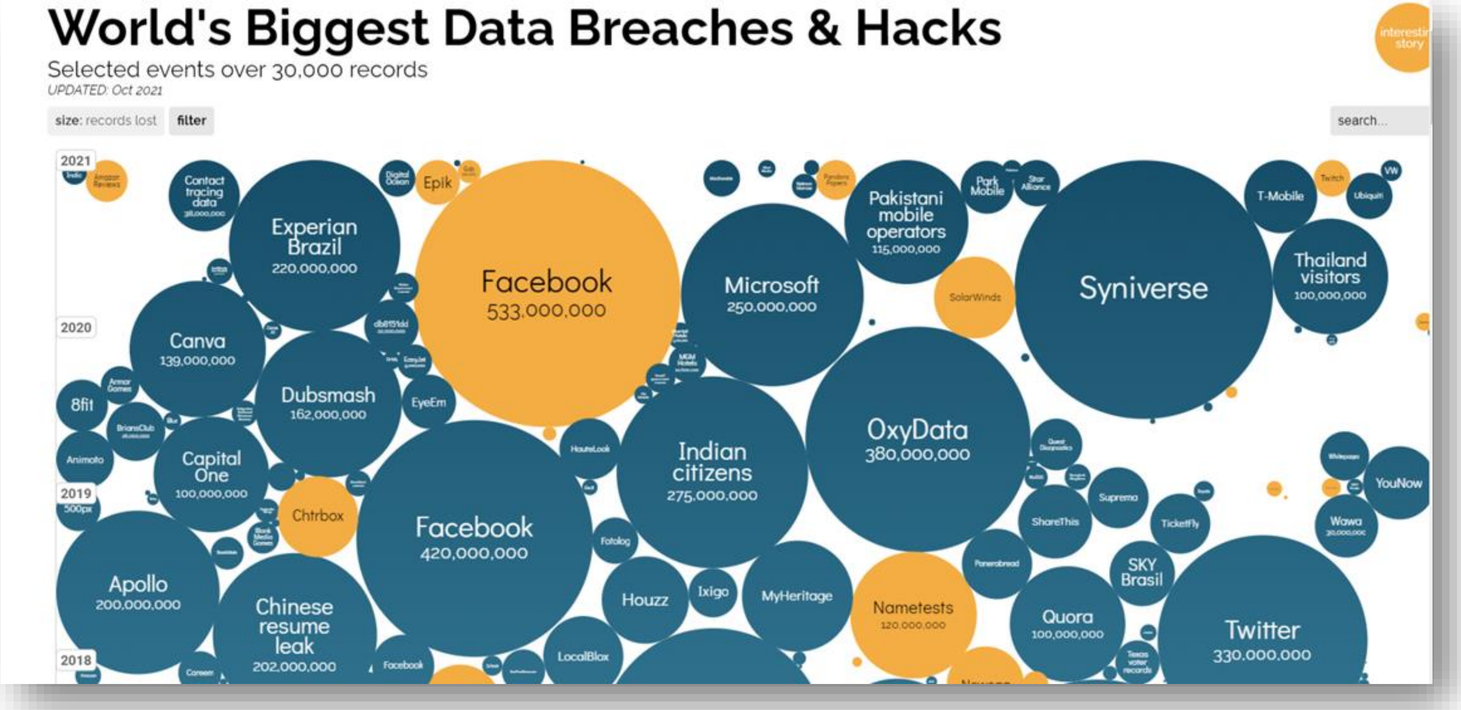
FOR IMMEDIATE RELEASE Tuesday, June 2, 2020

Nebraska Man Admits Stealing and Selling His Employer's Confidential Information

NEWARK, N.J. – A Nebraska man today admitted engaging in fraudulent activity that exposed his employer's confidential information, U.S. Attorney Craig Carpenito announced.

Data Breaches by the Numbers

44% of data breaches across SMBs are due to internal actors



World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

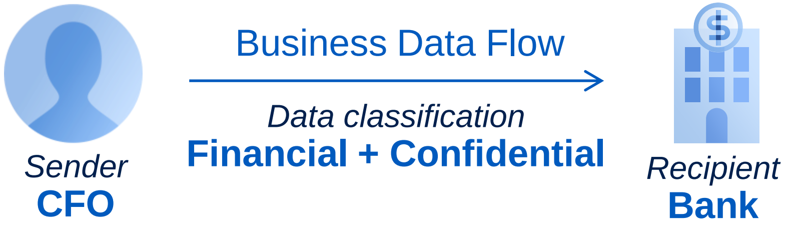
UPDATED: Oct 2021

size: records lost | filter

search...

Sources: New York Times, Forbes, The Guardian, Tech Radar, BBC, PC Mag, Tech Crunch, Informationisbeatiful.net, Verizron “SMB Data Breaches Deep Dive”, 2021

What is Data Loss Prevention (DLP)



Sender
CFO

Business Data Flow

Data classification
Financial + Confidential

Recipient
Bank

- **What is DLP?** - A system that blocks risky data flows that are unnecessary for the business.
  - **Analogy:** “plumbing system” for sensitive business data flows
- **What it does?** - Detects and prevents unauthorized use, transmission, and storage of confidential, protected or sensitive data.
- **How it does it?** - For any sensitive data transfer operation, detects its context (e.g. sender, recipient, channel used, data type) and content (what data is sent). Automatically applies controls, pre-defined in policies, based on the operations’ context and content

Acronis

#CyberFit

DLP Essentials

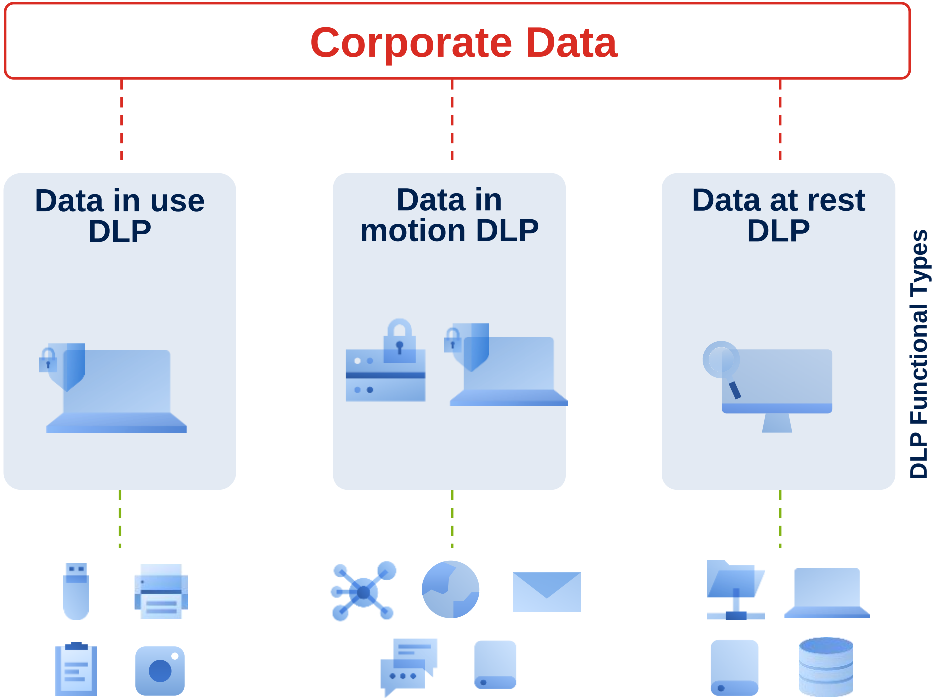
Data Types and How Different “Functional” DLPs Protect them

Data in use – data being used/transferred in local channels (e.g. peripherals, removable storage) / applications on endpoint computers

Data in motion – data transmissions in network communications

Data at rest DLP – data stored both locally or in a network

Functional DLPs are dedicated to protecting each of these types of data.



Acronis

#CyberFit

DLP Market

Overview

The Need for DLP

Insider-related threats

90% of **organizations feel vulnerable to insider threats**

72% of employees share sensitive, confidential or regulated company information

Traditional antiviruses, firewalls, or encryption do not protect against insider-related data leakage

Complexity of data protection

89% of security leaders report that they **lack visibility into data** that they need to protect

DLP solutions present the only technology capable of providing visibility into data flows across an organization

Compliance with regulations

54% of SMBs indicate a **top factor for IT investment decisions** is the “need to comply with regulations, laws, and other mandates” while **70% of breaches involve PII**

Data safeguard requirements **for cyber insurance** are covered by DLP

Leakage of data that is subject to regulations can lead to financial and reputational damage

Sources: “State of endpoint security risk,” Ponemon Institute, 2021; Security Leader’s Peer Report”, Panaseer, 2022; “Global Cost of Insider Threats”, Ponemon Institute, 2020; “Insider Threat Report”, Cybersecurity Insiders, 2018,

DLP Market Overview

DLP Market is heavily **focused on enterprises**

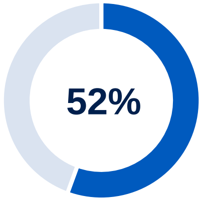
CAGR of 23.47% from 2021-2026

Top end-user industries:

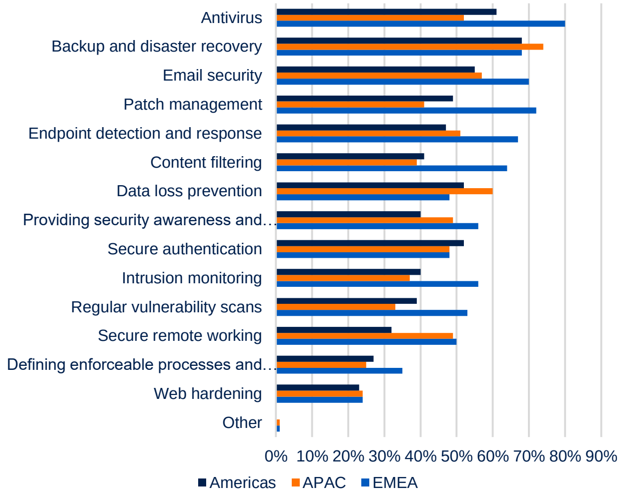
- IT providers and telecoms
- BFSI (Banking & finance)
- Government
- Healthcare – **expected significant growth**
- Manufacturing
- Retail and logistics

Largest market: North America
Fastest growing market: Asia Pacific

Top security services offered by MSPs



DLP services



73% of MSPs saw a revenue increase in the past year via security service offerings

Sources: Mordor Intelligence, 2021; "Information Security and Risk Management, Worldwide, 2018-2024", Gartner, Q4 2020 update; "2020 MSP BENCHMARK SURVEY RESULTS REPORT", Kaseya, 2020 . Datto – 2019 SMB Market Report for MSPs

Acronis

#CyberFit

Challenges with Current DLP Solutions

MSP Challenges with Traditional DLP Solutions

Conventional DLP solutions are not designed for MSPs and building services with them is costly

Launching a DLP service requires adding costly headcount

- Cybersecurity workforce gap is 3.1 million; 84% of organizations are experiencing an **IT security skills shortage**
- DLP experts are harder to find and more expensive compared to general IT security experts

DLP services provisioning complexity

- DLP solutions have **complex, manual processes** for policy creation and adjustment
- **69% of MSP technicians** spend more time managing tools than defending against threats
- **High labor cost** for MSPs

Efficient DLP requires business-specific policies

- Business processes and data sensitivity of any organization are unique – require **client-specific** DLP policy and data classifications
- **MSPs lack and can not acquire** such deep knowledge of clients' business specifics

Misconfigured DLP policies can disrupt business continuity

- Manual DLP policy creation and configuration is error-prone due to complexity and granularity
- Misconfigured DLP policies can block essential data flows and affect business continuity – thus increasing client churn

Lack of DLP solutions designed for small and mid-sized MSPs

- Traditional DLP solutions are not adjusted to business models of small MSPs
- DLP solutions for large MSSPs require costly consultancy from vendors not affordable for small and mid-size clients

Acronis

#CyberFit

Advanced DLP: Value for MSPs

Overview

A DLP Solution Built for MSPs

Business benefits of Advanced DLP

Challenge

Lack of DLP solutions designed for MSPs

- None of available DLP solutions are adjusted to small and mid-sized MSPs' business models

Launching DLP services is costly and complex

- DLP solutions have **complex, manual processes** for policy creation and follow-up adjustments

Employees are clients’ weakest link

- Human error is the number one factor for breaches.
  Yet, if client data is exfiltrated due to negligent or malicious employees, the MSP could suffer the reputational damage and churn

Solution

Unlock new profitability opportunities

- **Improve your revenue per client and attract more clients**
  MSP-managed DLP services previously available only in the enterprise market

Reduce complexity and free up resources

- **Reduce provisioning and management complexity** with automatic, client-specific policy creation

Mitigate data leakage risks for clients

- **Minimize clients’ insider-data breach risks** by detecting and preventing sensitive information leakage

Advanced DLP

Prevent leakage of clients' sensitive data

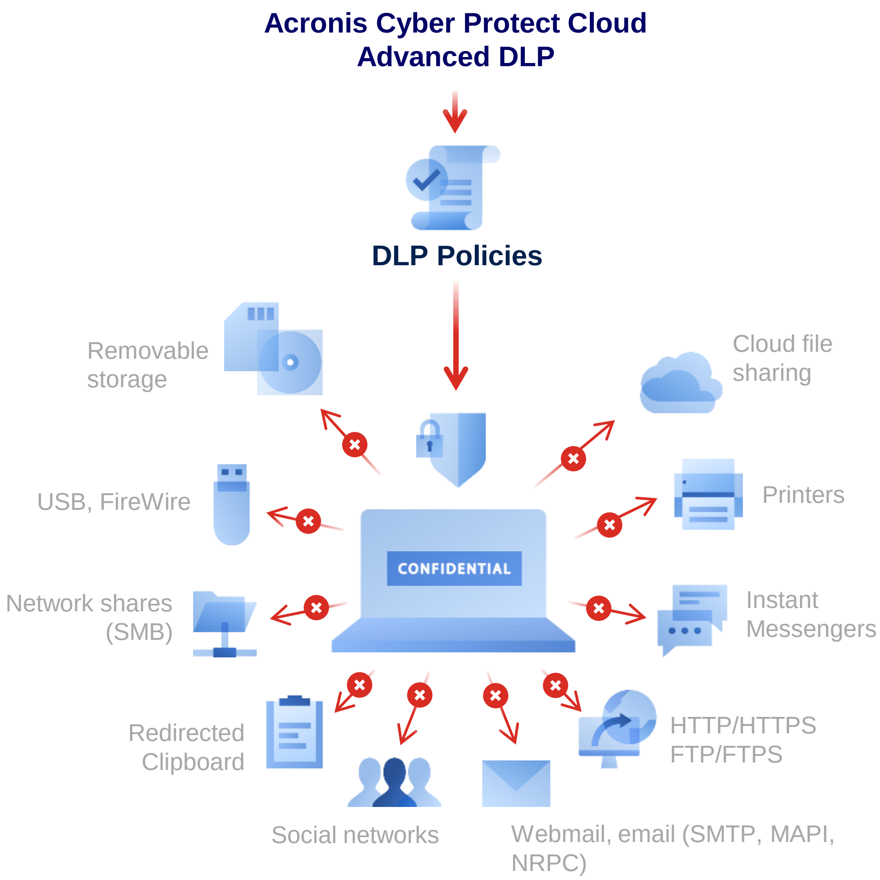
Analyze the content and context of data transfers via peripheral devices and network communications and enforce preventive controls, pre-defined in policies.

Automatically create client-specific baseline DLP policies

No need to drill down into client business details and define policies manually. Business-specific baseline DLP policies are created automatically by monitoring outgoing sensitive data flows.

Automate DLP policy enforcement

Minimize manual work usually needed to manage and adjust a DLP policy after initial enforcement. Automatically extend the enforced policy with new business-related data flow rules, detected on clients' workloads.



Automatic, Client-specific DLP Policy Generation

Simplified service provisioning and initial DLP policy configuration

Observation mode – monitor all sensitive data flows across clients' environment and create new rules in the initial DLP policy automatically. Allow only those data flows necessary to perform the business activities.

- Automatic initial DLP policy set up
- Optional end-user justification during initial DLP policy generation
- Effortlessly validate every data flow with clients prior enforcement

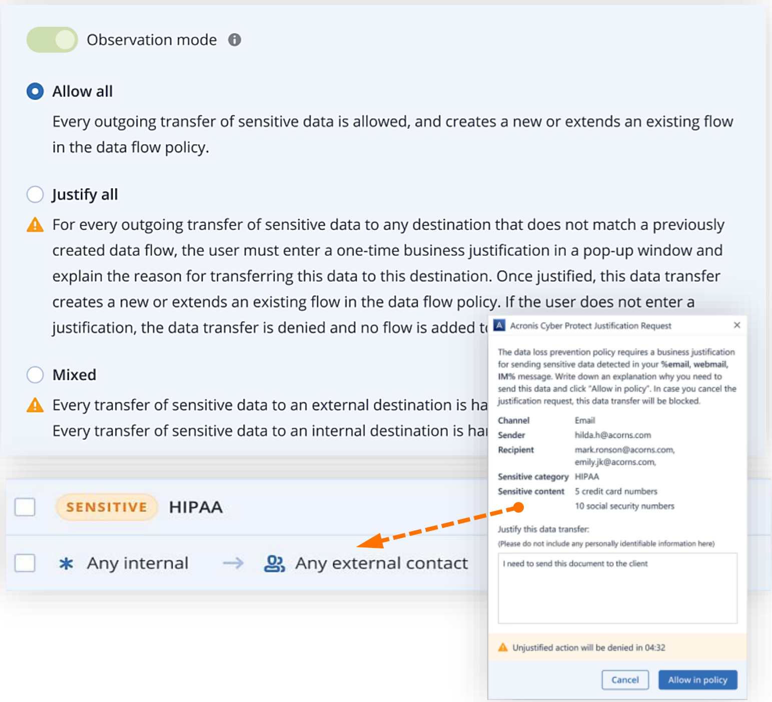
Example:

1. User sends HIPAA-related data to an external consultant via email (e.g. John.Doe@email,com)

2. The data flow is automatically added to the DLP policy as a rule (optionally, the user needs to enter a written justification)

3. All rules automatically created during the observation period are combined into the initial DLP policy.

4. Each rule in the policy is validated with the client prior enforcement



Observation mode

● Allow all

Every outgoing transfer of sensitive data is allowed, and creates a new or extends an existing flow in the data flow policy.

○ Justify all

⚠ For every outgoing transfer of sensitive data to any destination that does not match a previously created data flow, the user must enter a one-time business justification in a pop-up window and explain the reason for transferring this data to this destination. Once justified, this data transfer creates a new or extends an existing flow in the data flow policy. If the user does not enter a justification, the data transfer is denied and no flow is added t

○ Mixed

⚠ Every transfer of sensitive data to an external destination is ha
Every transfer of sensitive data to an internal destination is ha

□ SENSITIVE HIPAA

□ Any internal → Any external contact

Acronis Cyber Protect Justification Request

The data loss prevention policy requires a business justification for sending sensitive data detected in your **%email, webmail, IM%** message. Write down an explanation why you need to send this data and click "Allow in policy". In case you cancel the justification request, this data transfer will be blocked.

Channel	Email
Sender	hilda.h@acorns.com
Recipient	mark.ronson@acorns.com, emily.jk@acorns.com,
Sensitive category	HIPAA
Sensitive content	5 credit card numbers 10 social security numbers

Justify this data transfer:
(Please do not include any personally identifiable information here)

I need to send this document to the client

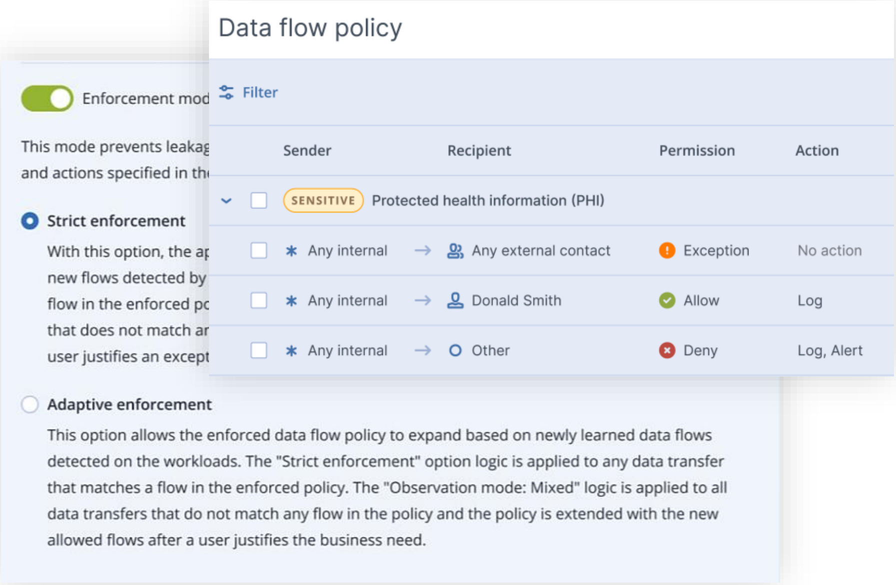
⚠ Unjustified action will be denied in 04:32

Automated, User-assisted DLP Policy Extension

Enable automatic enrichment of the enforced DLP policies by learning from end users

Enforcement mode (apply the validated DLP policy)

- Control data transfer operations that do not match any rule in the enforced policy
  - Strict enforcement – prevention of any new data flows that do not match already approved ones in the DLP policy
  - Adaptive enforcement – automated, user-assisted extension of enforced policies with new data flows



Enforcement mod

This mode prevents leakag and actions specified in th

● Strict enforcement

With this option, the ap new flows detected by flow in the enforced po that does not match ar user justifies an except

○ Adaptive enforcement

This option allows the enforced data flow policy to expand based on newly learned data flows detected on the workloads. The "Strict enforcement" option logic is applied to any data transfer that matches a flow in the enforced policy. The "Observation mode: Mixed" logic is applied to all data transfers that do not match any flow in the policy and the policy is extended with the new allowed flows after a user justifies the business need.

Data flow policy

Filter

	Sender		Recipient	Permission	Action
□	SENSITIVE Protected health information (PHI)				
□	✱ Any internal	→	Any external contact	Exception	No action
□	✱ Any internal	→	Donald Smith	Allow	Log
□	✱ Any internal	→	○ Other	Deny	Log, Alert

How Advanced DLP Differs from Competition?

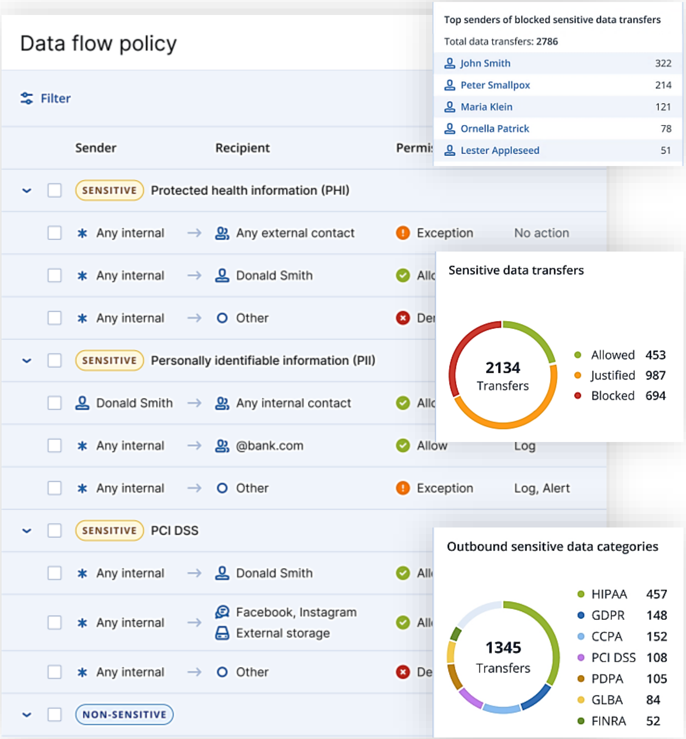
Automates DLP policy generation that learns from end users

Value:

- Ease service provisioning and policy configuration
- Minimize the risk of errors
- Simplify complexity to reduce hiring needs

How policies are created in traditional DLP solutions:

- Manual, complex, error-prone processes for DLP policy configuration
- Require costly consultancy from vendors



Data flow policy

Filter

	Sender		Recipient	Permi	
□	SENSITIVE Protected health information (PHI)				
□	Any internal	→	Any external contact	Exception	No action
□	Any internal	→	Donald Smith	Allo	
□	Any internal	→	Other	Der	
□	SENSITIVE Personally identifiable information (PII)				
□	Donald Smith	→	Any internal contact	Allo	
□	Any internal	→	@bank.com	Allow	Log
□	Any internal	→	Other	Exception	Log, Alert
□	SENSITIVE PCI DSS				
□	Any internal	→	Donald Smith	All	
□	Any internal	→	Facebook, Instagram External storage	All	
□	Any internal	→	Other	De	
□	NON-SENSITIVE				

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

Sensitive data transfers

2134 Transfers

● Allowed	453
● Justified	987
● Blocked	694

Outbound sensitive data categories

1345 Transfers

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

Easily enables client-specific DLP policy management

Value:

- Automatically map client's business processes to DLP policies
- Optional end-user assistance for higher accuracy and client validation before enforcing

How policies are created in traditional DLP solutions:

- Need to know clients' business specifics in-depth to map them to DLP policies
- MSPs can't acquire sufficient knowledge of each clients' business

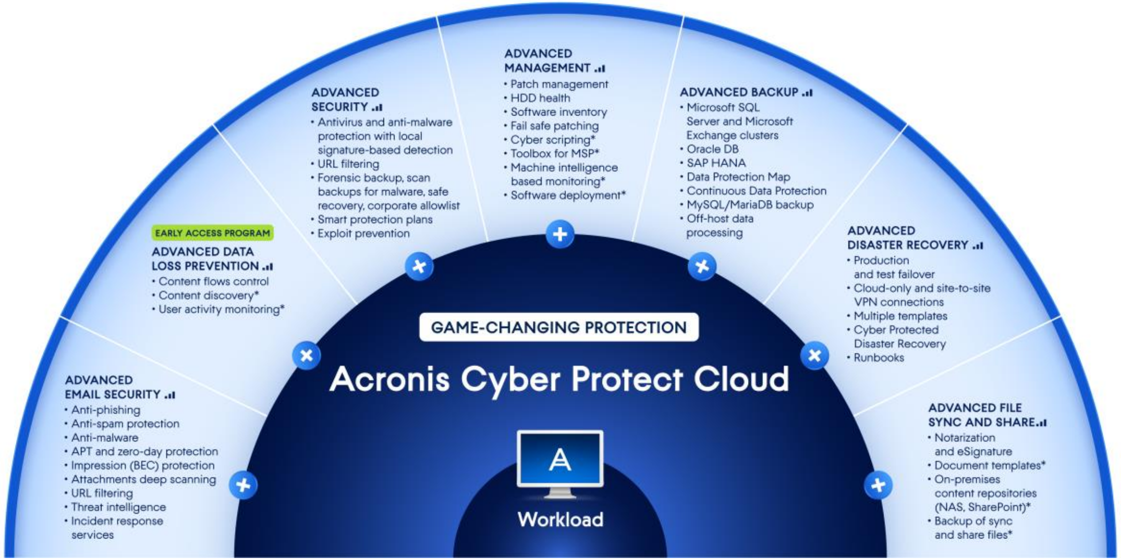
Acronis

#CyberFit

Licensing

Overview

Add advanced packs:
Security, Backup, Disaster Recovery, Email Security, File Sync and Share, Management **and now Data Loss Prevention**



ADVANCED MANAGEMENT
- Patch management
- HDD health
- Software inventory
- Fail safe patching
- Cyber scripting*
- Toolbox for MSP*
- Machine intelligence based monitoring*
- Software deployment*

ADVANCED SECURITY
- Antivirus and anti-malware protection with local signature-based detection
- URL filtering
- Forensic backup, scan backups for malware, safe recovery, corporate allowlist
- Smart protection plans
- Exploit prevention

ADVANCED BACKUP
- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection
- MySQL/MariaDB backup
- Off-host data processing

EARLY ACCESS PROGRAM

ADVANCED DATA LOSS PREVENTION
- Content flows control
- Content discovery*
- User activity monitoring*

ADVANCED DISASTER RECOVERY
- Production and test failover
- Cloud-only and site-to-site VPN connections
- Multiple templates
- Cyber Protected Disaster Recovery
- Runbooks

ADVANCED EMAIL SECURITY
- Anti-phishing
- Anti-spam protection
- Anti-malware
- APT and zero-day protection
- Impression (BEC) protection
- Attachments deep scanning
- URL filtering
- Threat intelligence
- Incident response services

ADVANCED FILE SYNC AND SHARE
- Notarization and eSignature
- Document templates*
- On-premises content repositories (NAS, SharePoint)*
- Backup of sync and share files*

GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

Workload

Optimize for every workload

Increase your service offerings and revenue per workload

Consolidate vendors

* Coming soon

Advanced DLP: Licensing

Advanced DLP will be applicable to both per-GB and per-workload licensing models

Advanced DLP will licensed as an Advanced pack for Acronis Cyber Protect Cloud.

During the Early Access Program, Advanced DLP is accessible for partners at no cost, enabling them to easily plan their service launch/upgrade

Pack	Features
Advanced DLP	Content / context-aware data loss prevention for workloads in local and network channels
	Automatic, client-specific baseline DLP policy generation
	Automatic end user profile creation and enrichment
	Pre-built data classifiers
	Adaptive DLP policy enforcement
	Policy-based centralized audit logging

Advanced DLP Early Access Program (EAP)

Early Access Program (EAP) Conditions

- Per-workload licensing in both per-workload and pe-GB billing modes
- Deployed in production Cyber Cloud
- Standard advanced pack enablement and provisioning (no program registration), regular support
- Partners deliver Advanced DLP Early Access as a service to their clients
- Partners are not charged for Advanced DLP during the EAP period
- Once the general availability version of Advanced DLP is launched, its use will become payable

Pack	Features
Advanced DLP	Content / context-aware data loss prevention for workloads in local and network channels
	Automatic, client-specific baseline DLP policy generation
	Automatic end user profile creation and enrichment
	Pre-built data classifiers
	Adaptive DLP policy enforcement
	Policy-based centralized audit logging

Acronis

#CyberFit

How to Position your Services with Advanced DLP to Clients?

Acronis

#CyberFit

Advanced DLP: Benefits

Value proposition

DLP Services that Bring Superior Protection to Clients Data

Benefits for MSP clients

Challenge

Risk of data leakage

- Insider-threats are the number one factor for data breaches. Negligent or malicious employees are the weakest links, through which data leaves clients' environments
- Clients are blind to current data leaks in their organization

Misconfigured DLP policies can disrupt productivity

- DLP policy creation and configuration is error-prone due to complexity and granularity

Regulatory compliance

- Sensitive data that is subject to regulations (e.g. GDPR, HIPAA, PCI-DSS, etc.) is targeted by attackers

Solution

Reduce risks data breach risks

- **Eliminate client insecurity** (financial/reputational loss) due to data leakage and implement the least privilege principle
- **Monitor, detect and report on** all sensitive data transfers and most risky users

Assure business-specific DLP policies

- **Automatically map DLP policies to clients' business specifics** with optional end-users assistance for higher accuracy
- **Easily validate policies with clients prior enforcement** (no technical know-how needed)

Strengthen regulatory compliance

- **Help client achieve compliance with regulations** HIPAA, GDPR, PCI-DSS, etc.

Acronis

#CyberFit

Advanced DLP: Overview

Value proposition

Protect your Sensitive Data

Help clients comply with regulations and reduce insider data breach risks

GDPR

Personally identifiable information (PII)

Prevent unauthorized disclosure of employees’ PII – name, email, address, SSN, passport number, drivers license, social media account, etc.

HIPAA
Health Insurance Portability
& Accountability Act

Protected health information (PHI)

Block sending a patient’s PHI from a medical center to external recipients or publishing PHI to social media

PCi

Payment card information (PCI DSS)

Avoid accidental or deliberate sharing of clients’ payment card data with contractors

CONFIDENTIAL

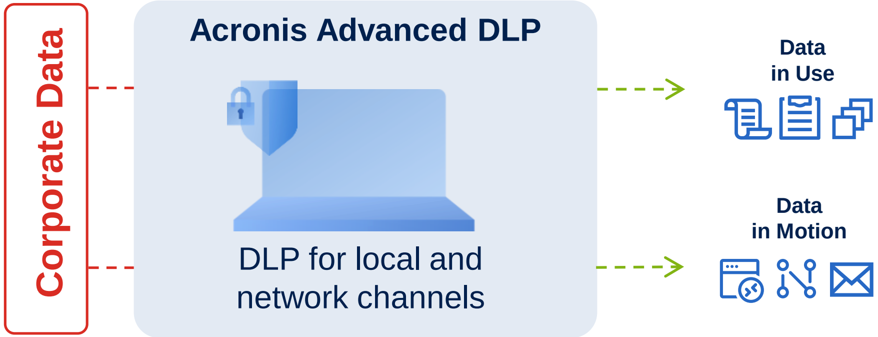
Documents marked as confidential

Prevent uploads of sensitive business documents with the “Confidential” watermark to employees’ private storage at file sharing services

Prevent Data Leaks Across Local and Network Channels

Block risky data flows across all channels

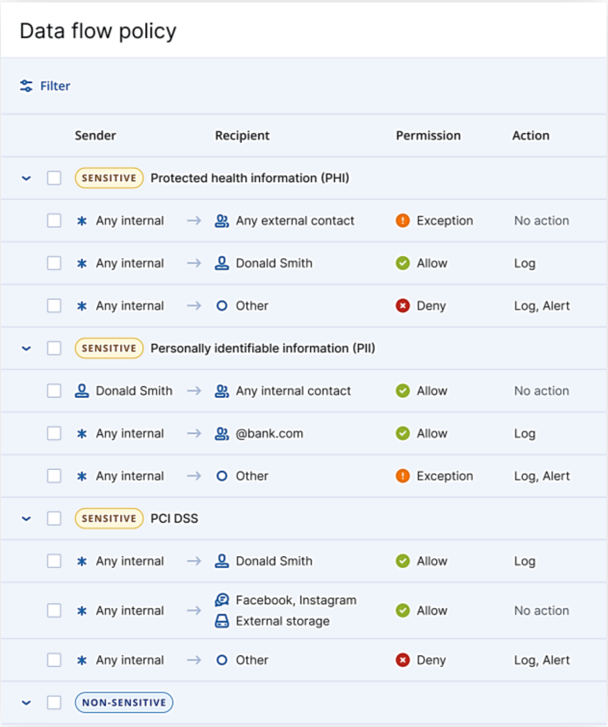
- **Local channels**
  - Removable storage
  - Printers,
  - Redirected mapped drives
  - Redirected clipboard
- **Network communications**
  - Emails – SMTP, Microsoft Outlook (MAPI), IBM Notes
  - 6+ Instant messengers
  - 15+ Webmail services
  - 28+ File sharing services
  - 15+ Social networks
  - File sharing, web access, and file transfer protocols
- **Protected workload types**
  - Physical and virtual machines running Windows 7 SP1+ and Windows Server 2008 R2+



Allow only Data Flows Necessary for the Business with High Level of Accuracy

Ensure business continuity

- **Assure business-specific DLP policies with high level of accuracy**
  - Create DLP policies by learning from end-users
  - Removed the human factor to increase policy accuracy
- **Minimize business disruptions**
  - **Easy validation with clients prior enforcement**. The validation requires no technical expertise from the client representative with whom the policy is reviewed – the DLP policy is displayed in an easy-to-understand graphical form
  - **Optional automated extension of enforced policies** with newly observed sensitive data flows
  - **Enable end users to override a data transfer block in case of extraordinary situations** by requesting a one-time business-related exception



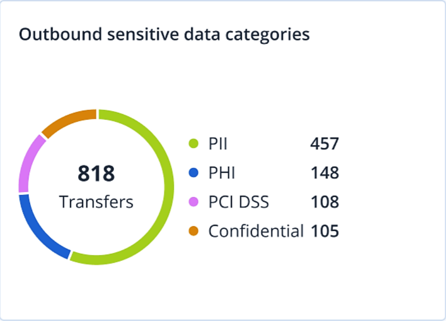
Data flow policy

Filter

Sender		Recipient	Permission	Action
SENSITIVE Protected health information (PHI)				
Any internal	→	Any external contact	Exception	No action
Any internal	→	Donald Smith	Allow	Log
Any internal	→	Other	Deny	Log, Alert
SENSITIVE Personally identifiable information (PII)				
Donald Smith	→	Any internal contact	Allow	No action
Any internal	→	@bank.com	Allow	Log
Any internal	→	Other	Exception	Log, Alert
SENSITIVE PCI DSS				
Any internal	→	Donald Smith	Allow	Log
Any internal	→	Facebook, Instagram External storage	Allow	No action
Any internal	→	Other	Deny	Log, Alert
NON-SENSITIVE				

Compliance Reporting to Clients

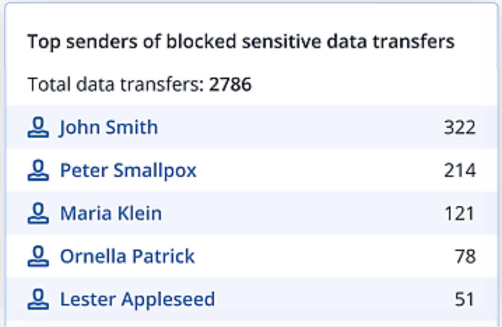
Information-rich widgets provide deeper visibility into DLP performance



Outbound sensitive data categories

818 Transfers

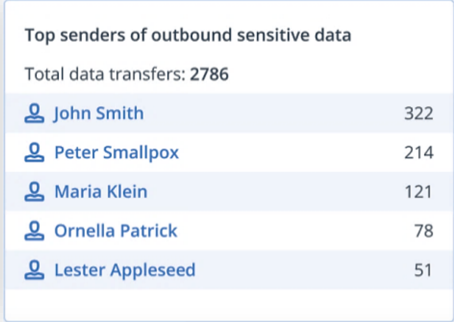
●	PII	457
●	PHI	148
●	PCI DSS	108
●	Confidential	105



Top senders of blocked sensitive data transfers

Total data transfers: **2786**

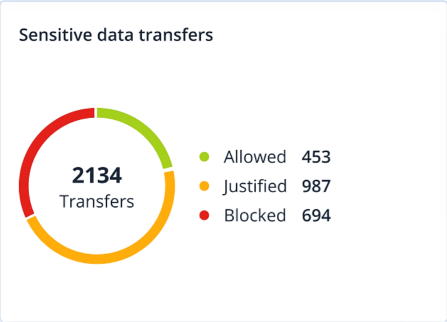
John Smith	322
Peter Smallpox	214
Maria Klein	121
Ornella Patrick	78
Lester Appleseed	51



Top senders of outbound sensitive data

Total data transfers: **2786**

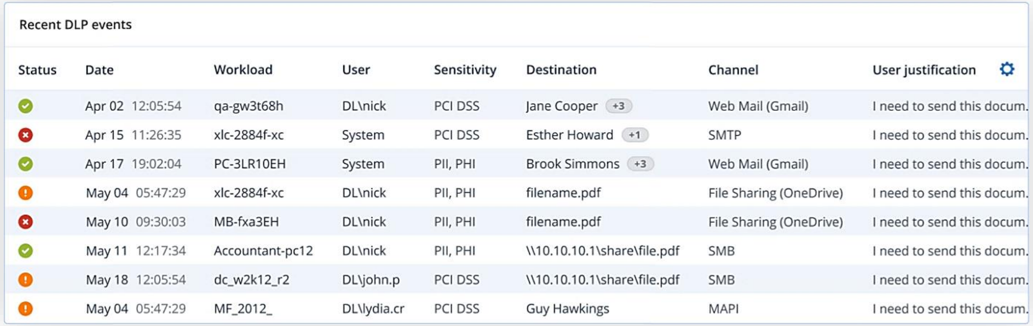
John Smith	322
Peter Smallpox	214
Maria Klein	121
Ornella Patrick	78
Lester Appleseed	51



Sensitive data transfers

2134 Transfers

●	Allowed	453
●	Justified	987
●	Blocked	694



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.

Acronis

#CyberFit

DLP Service Provisioning Flow

Timeline: How to Provision your Services with Advanced DLP

Activity	Average time spent
1. Initial service provisioning (Observation mode)	
• Remotely install the Acronis Cyber Protect Cloud agent on end-users' workloads, to deliver DLP services through it	**~ 1 hour**
• Initial DLP policy generation	**~ 1 – 2 months**
• Validation with clients prior enforcement	**~ 2 – 4 hours**
Total:	**~ 1 – 2 month(s)**
2. Follow-up policy enrichment and adjustments (Enforcement mode)	
• Automated enrichment of the enforced DLP policies with unobserved data flows by learning from end users	**N/A**
• Reporting on service value and validation of new DLP rules with clients prior enforcing them	**~ 1 – 3 hours / month**
Total	**~ 1 – 3 hours / month / client**

Keep in mind, that MSPs' client need to assign a business representative with knowledge of their organizations' business processes (non-technical knowledge) to validate the DLP policies prior enforcement.

Acronis

#CyberFit

How to Package Services with Advanced DLP?

Example: How to Package your Services with Advanced DLP

$49

Operational employee:

- ✅ Backup
- ✅ URL filtering
- ✅ Antivirus and malware protection

$79

Administrative office staff:

- ☑ Data loss prevention
- ✅ Backup
- ✅ URL filtering
- ✅ Antivirus and malware protection
- ✅ Email security
- Network security
- ✅ Hardware and software management
- Firewall
- Password management
- ✅ Patch management

$139

HR / Finance / Legal / Executive teams:

- ☑ Data loss prevention
- ✅ Backup
- ✅ URL filtering
- ✅ Antivirus and malware protection
- ✅ Email security
- Network security
- ✅ Hardware and software management
- Firewall
- Password management
- ✅ Patch management
- ✅ Drive health monitoring
- ✅ Continuous data protection
- ✅ Reporting
- ✅ File sync and share with e-signatures
- ✅ Disaster recovery

☑	Advanced DLP
✅	Acronis Cyber Protect Cloud / Other Advanced packs

Acronis

#CyberFit

Competitive Positioning

How to Differentiate your Services to Clients

Prevent all data flows unnecessary for the business and minimize disruptions

- Create **client-specific policies**, that are aligned with business needs by learning from end users
- Remove the human factor to make the DLP configuration process **less error-prone**
- **Minimize business disruptions**
  - Easy to validate with clients prior enforcement
  - Automatic policy extension with new data flows
  - One-time block override exceptions for extraordinary business needs

Control data flows across more channels than with competitors

Control data flows across local and network channels, including:

- Removable storage
- Printers
- Redirected mapped drives
- Redirected clipboard
- Emails
- 6+ Instant messengers
- 15+ Webmail services
- 28+ File sharing services
- 15+ Social networks
- Local file sharing, web access, and file transfer protocols

Address a broader scope of risks than with other DLP services

- Control data transfers to social media, webmail and file-sharing services **across any browser** – including not only files but also **webforms**, **messages**, and **posts**
- Detect and prevent leakage of **sensitive data in a graphical form,** including from remote and offline computers
- Inspect the **content** of outgoing **instant messages**
- Prevent data leakage via **any email desktop application**

Acronis

#CyberFit

Qualification Questions and Objection Handling

Advanced DLP

Conversation starters

For clients already managed by the MSP

Open ended questions	Notes
What would it mean for your business to get ongoing reporting on your compliance posture? Would this reduce the security risk of internal threats?	
Do you store sensitive data you need to protect?	Look for: Payment card data, client/employee personally identifiable information (PII), patient health information (PHI), intellectual property (IP), confidential information, trade secrets, state classified data
Which regulations do you need to be compliant with? Which ones do you find the most challenging to stay compliant with?	GDPR – personally identifiable information (PII) HIPAA – patient health information (PHI) PCI DSS – payment card data CCPA - personally identifiable information (PII)
Do you have a cyber insurance?	You can lower your cyber insurance premiums with better protection for data.
What do you imagine would be the impact for your business in case of a data leak?	Explain how this easy-to-launch new service will help reduce this risk while ensuring business continuity.
Is your business interested in getting some additional compliancy certificates in the near future?	Explain how DLP helps achieve regulatory compliance.

Conversation Starters

For clients managed by competitive MSPs

Open ended questions	notes
Have you been aware of data leaks in your organization? Do you think you have blind spots in your organization?	Explain that maybe current security services managed by the current MSP are not addressing all risks, especially in terms of regulatory compliance and sensitive data protection. With Acronis DLP you are addressing sensitive data leakage risks and strengthening your business resilience with minimal productivity disruption.
What do you imagine would be the impact for your business in case of a data leak?	
What would it mean for your business to get ongoing reporting on your compliance posture? Would this reduce the security risk due to internal threats?	
Which regulations do you need to be compliant with? Which ones do you find the most challenging to stay compliant with?	GDPR – personally identifiable information (PII) HIPAA – patient health information (PHI) PCI DSS – payment card data CCPA - personally identifiable information (PII)
Have you experienced data breaches in the past? What was the reason for them? How did it impact your business?	Explain that the data loss prevention services can help reduce the risk of data being leaked, even if threats get past other security layers.
Do you have a cyber insurance?	You can lower your cyber insurance premiums with better protection for data.
Is your business interested in getting some additional compliancy certificates in the near future?	Explain how DLP helps achieve regulatory compliance.

Conversation Starters

For clients whose IT was managed internally and are now looking to outsource it

Open ended questions	notes
How did your IT know if there were data leaks in your organization?	Talk about that other preventive layers (e.g. antimalware, email security, URL filtering) are not enough to stop data leaks and that you're blind to the threats that have bypassed such defenses. (e.g. malicious or negligent employees, undetected threats)
Given the maturity / security level of your IT staff, would you say you are comfortable creating and managing data loss prevention rules for all data flows across your organization on your own?	Help understand the need and see the service as valuable.
Do you feel your business is prepared to detect and block data leaks?	Explain anti-malware services are not enough to stop data leaks.
What technologies are you currently utilizing to protect your business?	See whether the client has only essential endpoint protection in place and explain why they're insufficient. Check if they have experience with utilizing encryption/archiving/data loss prevention.
What do you imagine would be the impact for your business in case of a data leak? Have you had similar experience in the past? Have your heard about companies in your industry who had?	Explain DLP services reduce the risks and increase business resilience, while providing you with actionable statistics related to your compliance posture
What would it mean for your business to get ongoing reporting on your compliance posture? Would this reduce the security risks due to internal threats?	
If you've managed a DLP on your own in the past, what were your biggest challenges?	Explain that with your DLP services built on top of Acronis: • The DLP policies are client-specific and easily-verifiable by client without technical expertise • You allow only data flows necessary for the business with high accuracy and reduced room for error • You ensure business continuity and reduce the risks of disruptions with automated extension of DLP policies with additional rules for newly observed data flows and optional one-time user justification

Conversation Starters (cont'd)

For clients whose IT was managed internally, and are now looking to outsource it

Open ended questions	notes
Have you been aware of data leaks in your organization? Do you think you have blind spots in your organization?	Explain that maybe current security services managed by the current MSP are not addressing all risks, especially in terms of regulatory compliance and sensitive data protection. With Acronis DLP you are addressing sensitive data leakage risks and strengthening your business resilience with minimal productivity disruption.
Do you have a cyber insurance?	You can lower your cyber insurance premiums with better protection for data.
Is your business interested in getting some additional compliancy certificates in the near future?	Explain how DLP helps achieve regulatory compliance.

Objection Handling

Question	Answer
I am already using anti-malware/firewall services. I thought I was protected, why do I need something on top?	▪ Endpoint protection services (antimalware, firewall) help to stop threats from reaching your network and data. ▪ However, they cannot protect you against attempts to exfiltrate your sensitive data – either by threats that have bypassed your defenses or by malicious or negligent insiders ▪ **Only DLP technologies can protect against data leaks**
We're utilizing a backup and recovery technology in our service stack to protect against clients' data loss. Why do I need to consider a DLP technology?	▪ Backup services guarantee your data is stored and recoverable, however, they do not protect sensitive data from being transferred to unauthorized recipients outside or inside the organization. ▪ **Only DLP technologies can protect against data leaks**
I am looking into other DLP services as well. Why do I need to consider yours? / How does your DLP service compare against other MSPs?	• There are many DLP services out there, but you need to consider which one strengthens your business resilience the most while also ensuring your business continuity and controlling costs • Competitive differentiators of our service (with Acronis): • Client specific policies with higher level of accuracy compared to manual configuration (other DLP services) • Easy validation with clients of the DLP policy prior enforcement. No technical knowledge is required from clients • Minimal business disruptions (automatic enhancement of enforced policy with additional rules for new, end-user-justified business data flows) • Reduced incident cost and strengthened compliance

Objection Handling (cont'd)

Question	Answer
How can I validate the DLP policy with my MSP when I do not have technical know-how?	▪ The initial DLP policy we will create and will be presented in an easy-to-understand graphical form. ▪ You can easily review and approve or choose to prohibit each sensitive data flow in the initial DLP policy ▪ You don't need a security know-how to validate whether a data flow is necessary for your business, you only need to know your business specifics
We have tried using DLP services in the past but we had business continuity issues. On top, it was too costly service. Why should we consider your service?	• Better accuracy due to: • Automation, less error-prone, based on learning from end-user business communications • Easy validation with client prior enforcement • Minimal disruptions with automated enhancement of enforced DLP policy with additional rules for new, end-user-justified data flows

Acronis
Cyber Foundation

Building a more knowledgeable future

Create, Spread and Protect Knowledge With Us!

- Building new schools
- Providing educational programs
- Publishing books

www.acronis.org

#CyberFit

Acronis

#CyberFit

Appendix

Acronis

#CyberFit

DLP Glossary

Advanced DLP

DLP glossary (1)

- **Administrative log** – an audit log of all administrative actions for managing and using DLP Logging Subsystem performed by its users with administrative privileges (roles) on backend Advanced DLP Service.
- **Agent log** – an audit log of all types of DLP agent service-specific events on managed DLP agents including agent start/stop, policy changes, local storage issues, etc.
- **Audit log / event log** – a log of records with parameters of events generated on managed DLP agents on end user-initiated operations controlled by DLP policies (such as access to peripheral devices or network communications, transferring data with sensitive content with or without policy violations, etc.).
- **Confidentiality** – preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Data loss (data leak)** – a breach of security in which sensitive data is accidentally or deliberately released to an untrusted environment or unauthorized users outside or inside the organization.
- **Data loss prevention (DLP)** – an information security technology that allows you to automatically detect and prevent unauthorized use, transmission, and storage of sensitive data.
- **DLP system** – a system of integrated information security technologies that automatically detects and prevents unauthorized use, transmission, and storage of sensitive data by applying a combination of contextual controls and content analysis methods to enforce acceptable data use policies used in the organization
- **DLP agent** – the built-in DLP software module of Acronis Cyber Protect Agent.

DLP glossary (2)

- **Data at rest DLP** – a function of DLP systems that discovers exposed sensitive content in data stored on corporate IT assets (e.g. network file shares, endpoint file systems, databases, document repositories, and cloud-based storage) and remediates data storage policy violations.
- **Data in motion DLP** – a function of DLP systems that prevents data leakage through network communications (e.g. emails, webmails, IMs, social media, cloud-based file sharing, as well as HTTP(S), FTP(S), and SMB protocols).
- **Data in use DLP** – a function of DLP systems that prevents data leakage through local channels, peripheral devices, and applications on protected endpoint computers (e.g. removable/fixed/redirected storage, Clipboard, printing, screenshot)
- **DLP policy –** a set of rules used by DLP agents for inspecting monitored data transfer operations in order to detect the sensitivity category of data being transferred, check whether the rule conditions are met and enforce their permissions and actions over controlled operations.
- **Data flow (business data flow) –** a generalized description of a business-related data transfer originating in the organization in terms of its sender (source), its recipient (destination) inside or outside the organization, and the sensitivity of transferred data. In DLP policy rules, a data flow is used as a condition and represents all particular data transfers that have the same sender, recipient, and data sensitivity as this flow. In policy rules, a data flow is used as a condition and represents all particular data transfers that have the same sender, recipient, and data sensitivity as in this flow.
- **Data flow policy –** a data loss prevention policy representation as a set of rules that collectively specify all allowed and prohibited sensitive data flows in the organization.

DLP glossary (3)

- **Data flow rule (data flow policy rule)** – a DLP policy rule format that specifies preventive and other controls uniformly enforced over one or more data flows with fully identical senders (sources), recipients (destinations), and sensitivity categories (classifications) of transferred data. A data flow rule contains information on the senders (sources), recipients (destinations), and sensitivity categories (classifications) of all data flows it controls, whether these data flows are allowed or prohibited, and a set of actions to be automatically performed if an intercepted data transfer triggers this rule.
- **End user** – a user of a workload (endpoint computer) protected by a DLP agent running on this workload.
- **Endpoint DLP** – a DLP system type that uses DLP agents only on endpoint computers. Endpoint DLP agents prevent data leaks from their host computers via both local and network channels regardless whether the endpoints are used inside the corporate network or in the Internet. Endpoint DLP also supports content discovery and remediation in local file systems of computers with DLP agents, as well as on local file shares accessible form these computers.
- **Hybrid DLP** – a DLP system type that utilizes both network and endpoint DLP components, as well as performs all functions of both endpoint and network DLP types.
- **Network DLP** – a DLP system type that uses only network-resident components, including hardware/virtual DLP gateways and servers. They prevent data leaks via external network communications of computers located inside the corporate network. They can also discover and remediate sensitive content stored on local network shares, NAS, data repositories, and databases in the corporate network, as well as in cloud-based file sharing services.

DLP glossary (4)

- **Sensitivity** – a measure of the importance assigned to information (data) by its owner, for the purpose of denoting its need for protection.
- **Sensitive data (information)** – data (information) whose loss, misuse, or unauthorized access, disclosure or modification could adversely affect its owner (an organization or an individual). In the DLP context, sensitive data require protection against unauthorized use, transmission, and storage.
- **Sensitive data type/category (sensitivity type/category)** – a type of sensitive data distinguishable by its owner from other types of sensitive data for the purposes of using and protecting this data (e.g. “financial data”, “trade secrets”, PII).