Acronis

#CyberFit

Advanced Data Loss Prevention

A game-changing solution that prevents from data leakage

Advanced pack of Cyber Protect Cloud

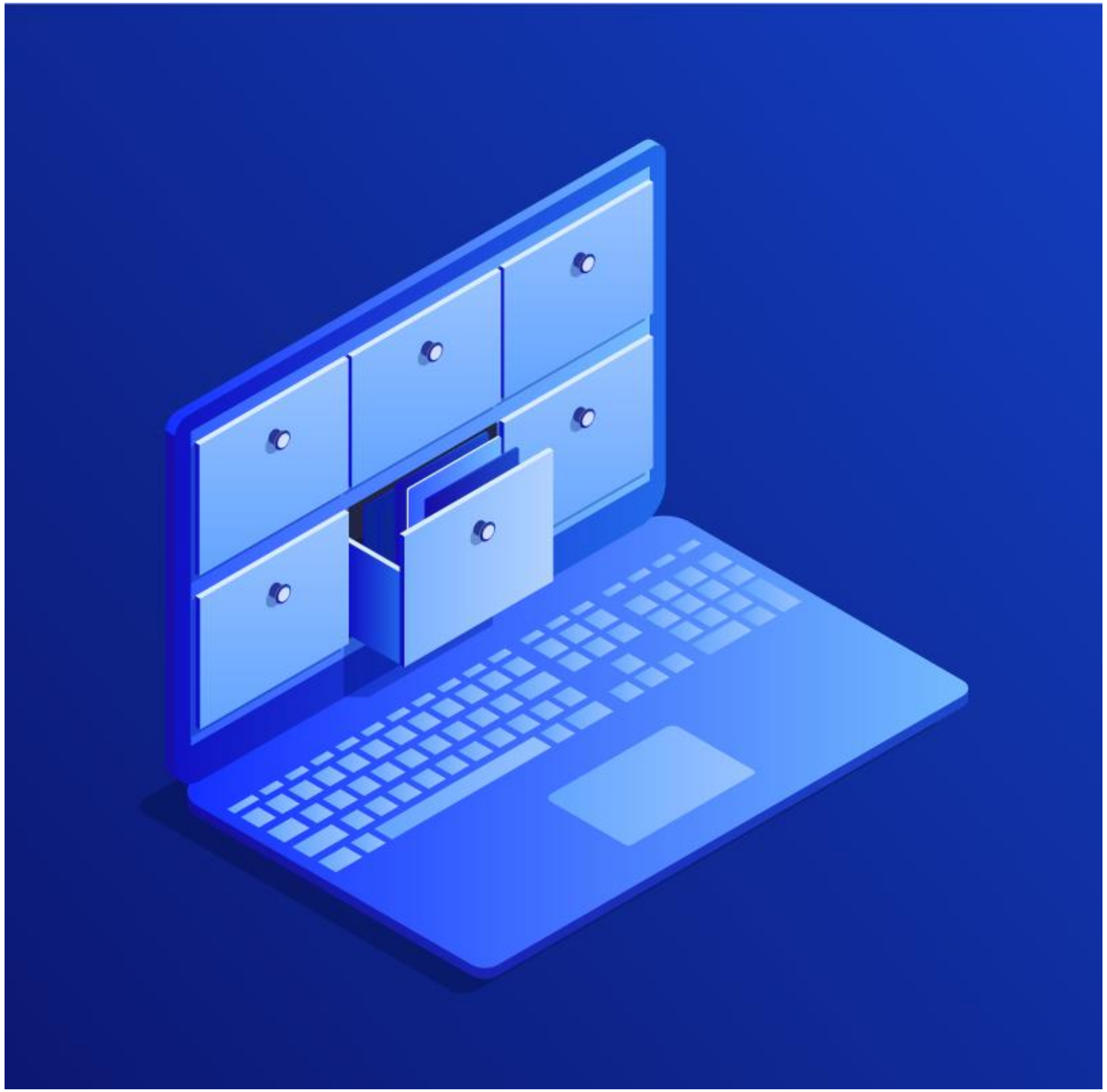
Early access

Agenda

1. Acronis Cyber Protect Cloud with Advanced Packs - overview
2. DLP essentials
3. Challenges with current DLP solutions
4. Advanced DLP: Benefits
5. Advanced DLP: Overview
6. Competitive positioning

7 Licensing

8. How to provision DLP services to clients

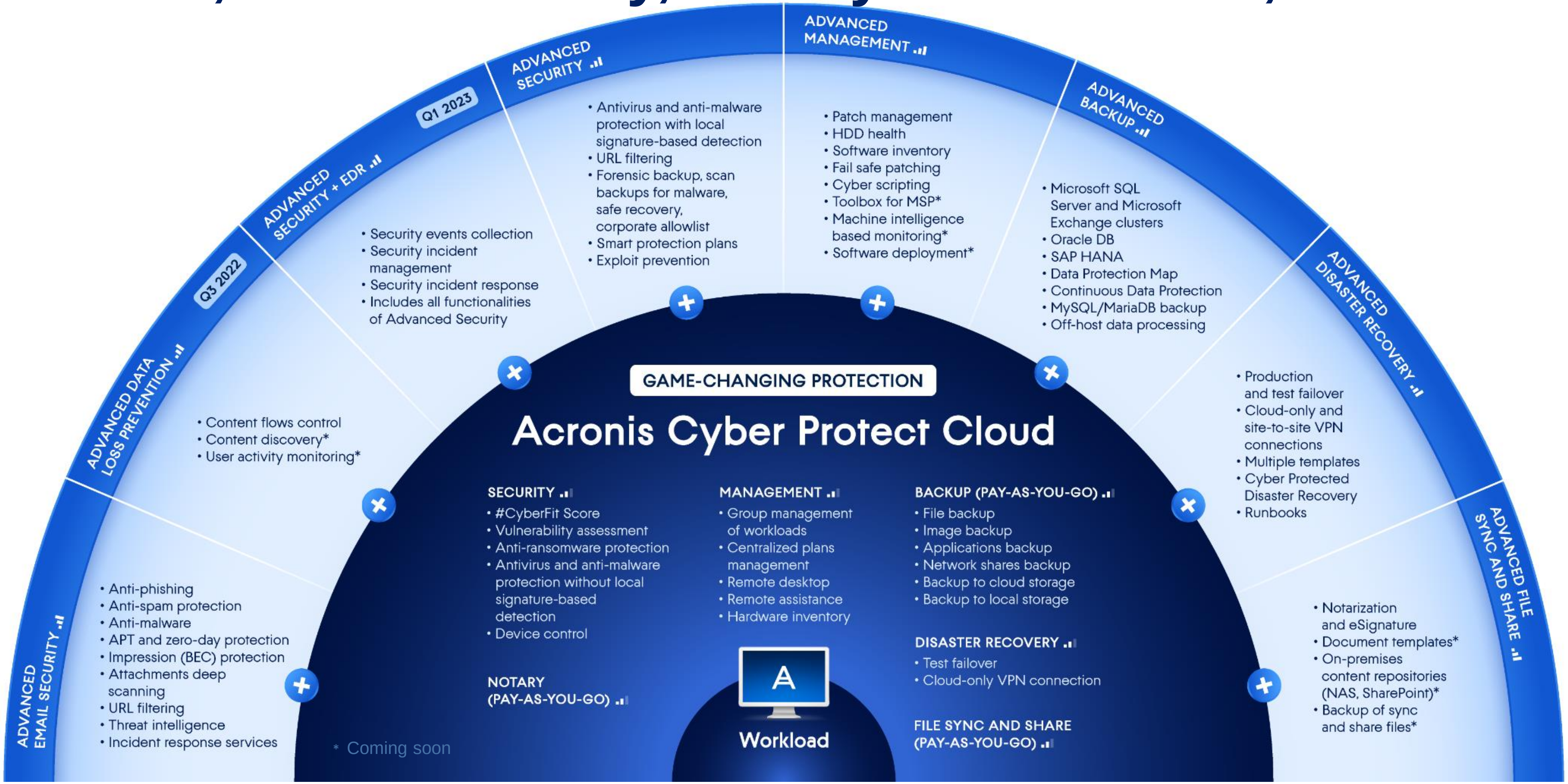


Acronis

#CyberFit

Acronis Cyber Protect Cloud with Advanced Packs

Advanced packs: Security, Management, Backup, DR, Email Security, File Sync and Share, DLP



GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

SECURITY
- #CyberFit Score
- Vulnerability assessment
- Anti-ransomware protection
- Antivirus and anti-malware protection without local signature-based detection
- Device control

NOTARY (PAY-AS-YOU-GO)

MANAGEMENT
- Group management of workloads
- Centralized plans management
- Remote desktop
- Remote assistance
- Hardware inventory

BACKUP (PAY-AS-YOU-GO)
- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY
- Test failover
- Cloud-only VPN connection

FILE SYNC AND SHARE (PAY-AS-YOU-GO)

Workload

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 DATA LOSS PREVENTION Q3 2022
- Content flows control
- Content discovery*
- User activity monitoring*

ADVANCED SECURITY + EDR Q1 2023
- Security events collection
- Security incident management
- Security incident response
- Includes all functionalities of Advanced Security

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

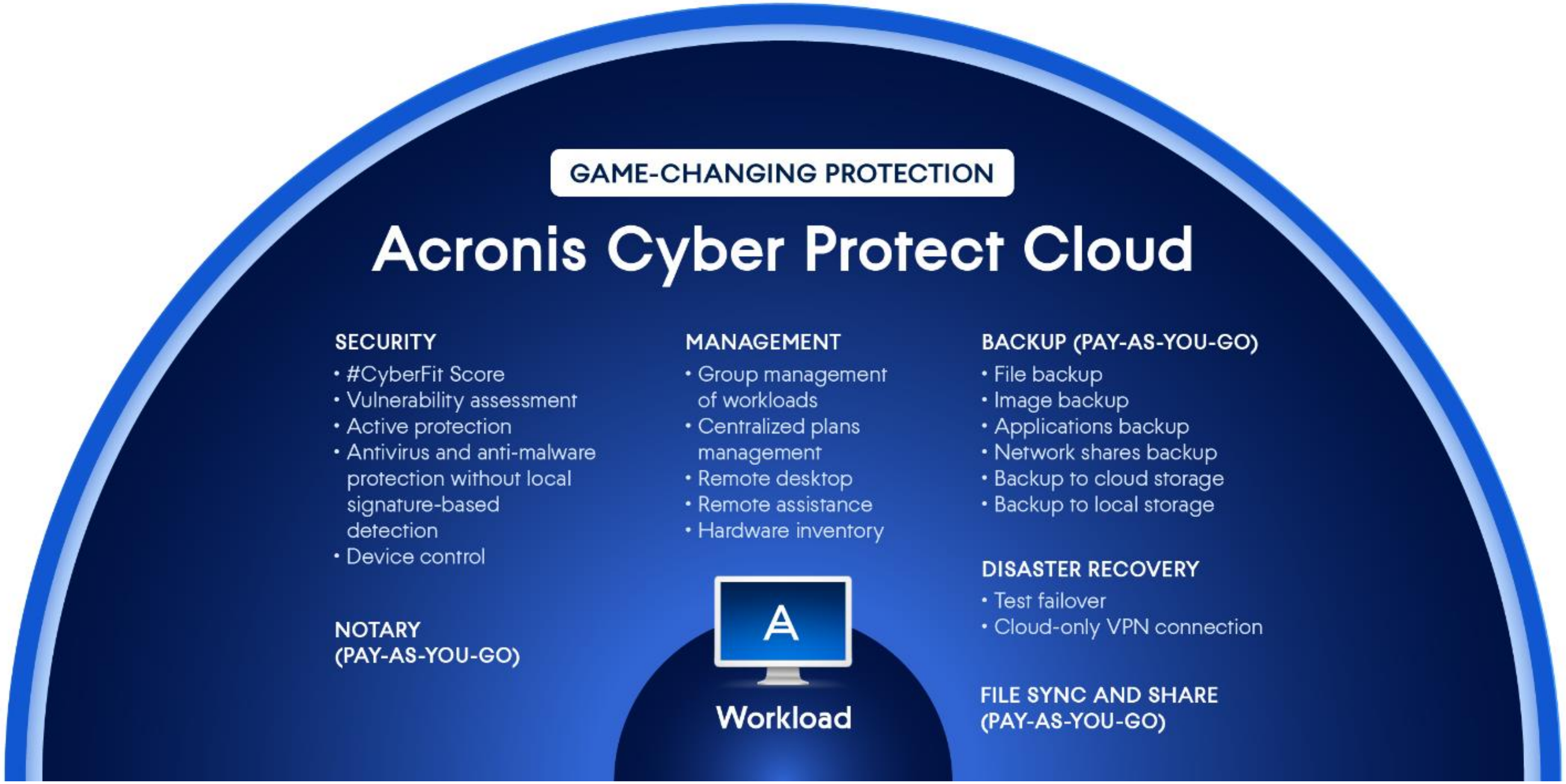
ADVANCED BACKUP
- Microsoft SQL Server and Microsoft Exchange clusters
- Oracle DB
- SAP HANA
- Data Protection Map
- Continuous Data Protection
- MySQL/MariaDB backup
- Off-host data processing

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

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

* Coming soon

Best-in-breed backup combined with integrated security and management



GAME-CHANGING PROTECTION

Acronis Cyber Protect Cloud

SECURITY

- #CyberFit Score
- Vulnerability assessment
- Active protection
- Antivirus and anti-malware protection without local signature-based detection
- Device control

NOTARY (PAY-AS-YOU-GO)

MANAGEMENT

- Group management of workloads
- Centralized plans management
- Remote desktop
- Remote assistance
- Hardware inventory

BACKUP (PAY-AS-YOU-GO)

- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY

- Test failover
- Cloud-only VPN connection

FILE SYNC AND SHARE (PAY-AS-YOU-GO)

Protect every workload at no charge

Best-in-breed backup included

Strengthens your AV against zero-day threats

Accelerate security and manageability

Acronis Cyber Protect Cloud with Advanced Backup

Protect your clients’ data confidently with best-in-breed backup enhanced with cyber protection

Increase automation and productivity

Scheduled backup reports, paired with cloud backup enhancements – like **continuous data protection** – helps you save time while saving your clients from data loss

Deliver the most secure backup

Acronis delivers a unique approach by **combining cloud backup with cyber protection features**, such as antimalware and antivirus – helping you keep clients’ data secure

Protect more workloads on more platforms

From a single console, protect more than 20 workload types, including **Microsoft Exchange, Microsoft SQL Server, Oracle DBMS Real Application clusters, and SAP HANA**

Advanced Disaster Recovery

Disaster recovery functionality

Network management

- Cloud-only mode
- Site-to-site Open VPN connection
- Multi-site IPsec VPN connection

Runbooks

- Creating a runbook
- Operations with runbooks

Cloud server management

- Creating a recovery server
- Testing a failover
- Performing a failover
- Performing failback to a virtual machine
- Performing failback to a physical machine
- Creating a primary server

Acronis Cyber Protect Cloud with Advanced Security

Improve security by detecting more threats, save on simplified security management, and deliver better remediation with integrated cyber protection

Full-stack antimalware

Acronis Active Protection, enhanced with exploit prevention, URL filtering, antimalware detection for backed-up data, and improved detection rate to catch more threats faster

Security automation

Smart protection plans, auto-allowlist custom apps, automatic malware scans and AV definitions updates as part of recovery process to deliver services more effortlessly

Efficient forensics

Collect digital evidence and safe it in a secure central repository to enable thorough post-incident investigations and proper remediation, while keeping costs down.

Acronis Cyber Protect Cloud with Advanced Management

Improve clients’ protection by keeping systems up-to-date while decreasing the management burden and TCO

Advanced patch management

Keep systems up-to-date and proactively mitigate vulnerabilities.

Patch management automation

Save time and effort with patch management automation and fail-safe patching technology

Comprehensive management tools

Streamline your planning with software inventory collection, report scheduling, and drive health monitoring.

Acronis Cyber Protect Cloud with Advanced Email Security powered by PERCEPTION POINT

Improve client security by detecting any email-borne threat before it reaches end-users

Stop phishing and spoofing attempts

Minimize risk for clients with powerful threat intelligence, signature-based detection, URL reputation checks, unique image-recognition algorithms, and machine learning with DMARC, DKIM, and SPF record checks.

Catch advanced evasion techniques

Detect hidden malicious content by deep scanning 100% of the traffic – recursively unpacking embedded files and URLs and separately analyzing them with dynamic and static detection engines.

Prevent APTs and zero-day attacks

Prevent advanced email threats that evade conventional defenses with Perception Point's unique CPU-level technology, which acts earlier in the attack chain to block exploits before malware is released, delivering a clear verdict within seconds.

*Product UI supports English only

Acronis Cyber Protect Cloud with Advanced Data Leakage Prevention

Prevent sensitive data leakage from end customer workloads via local and network channels

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.

Acronis

#CyberFit

Advanced Data Loss Prevention (DLP)

Early access

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?

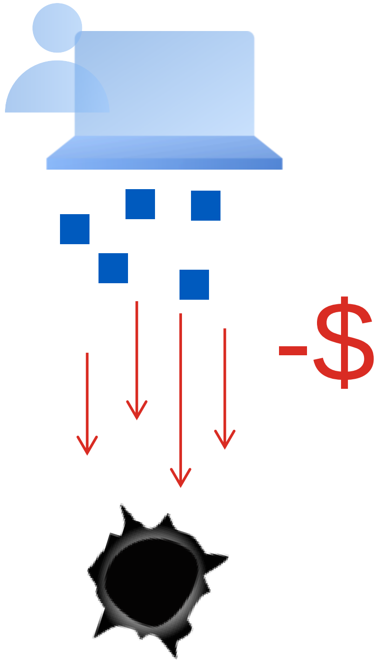
- Payment card data, client/employee personally identifiable information (PII), patient health information (PHI), intellectual property (IP), confidential information, trade secrets, state classified data…

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?

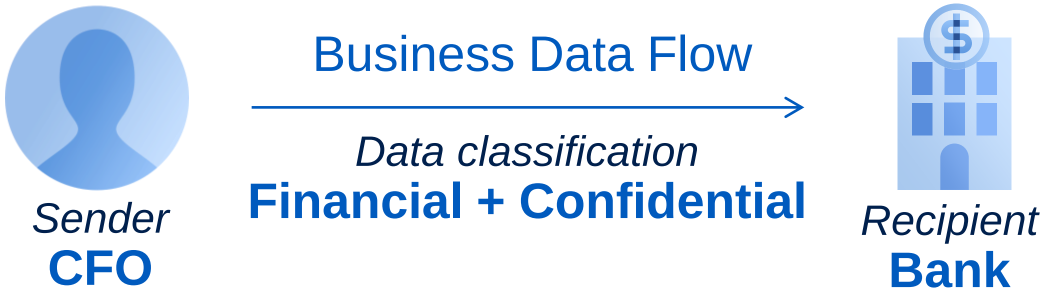
- Financial and reputational damages, loss of business
- Large fines and expensive litigations
- Damage to national security



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

What is data loss prevention (DLP)



Business Data Flow

Data classification

Financial + Confidential

Sender

CFO

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

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,

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: Benefits

Value proposition

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** with 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

A DLP solution built for MSPs (cont’d)

Technical benefits of Advanced DLP

Challenge

DLP service provisioning is complex

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

Efficient DLP requires business-specific policies

- Business processes and data sensitivity of any organization are unique – always require **client-specific** DLP policies
- **MSPs lack and can not acquire** such deep knowledge of clients’ business specifics to map them to DLP policies

Misconfigured DLP policies can disrupt productivity

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

Solution

Speed up service provisioning and management

- **Automate DLP service provisioning, initial policy configuration and follow-up adjustments**

Ensure client-specific DLP policies with minimal manual involvement

- **DLP policies are automatically aligned with business processes** with optional end-users assistance for increased accuracy
- **Easy client validation prior policy enforcement**

Minimize human errors

- **Minimize the impact of human errors** through automation

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

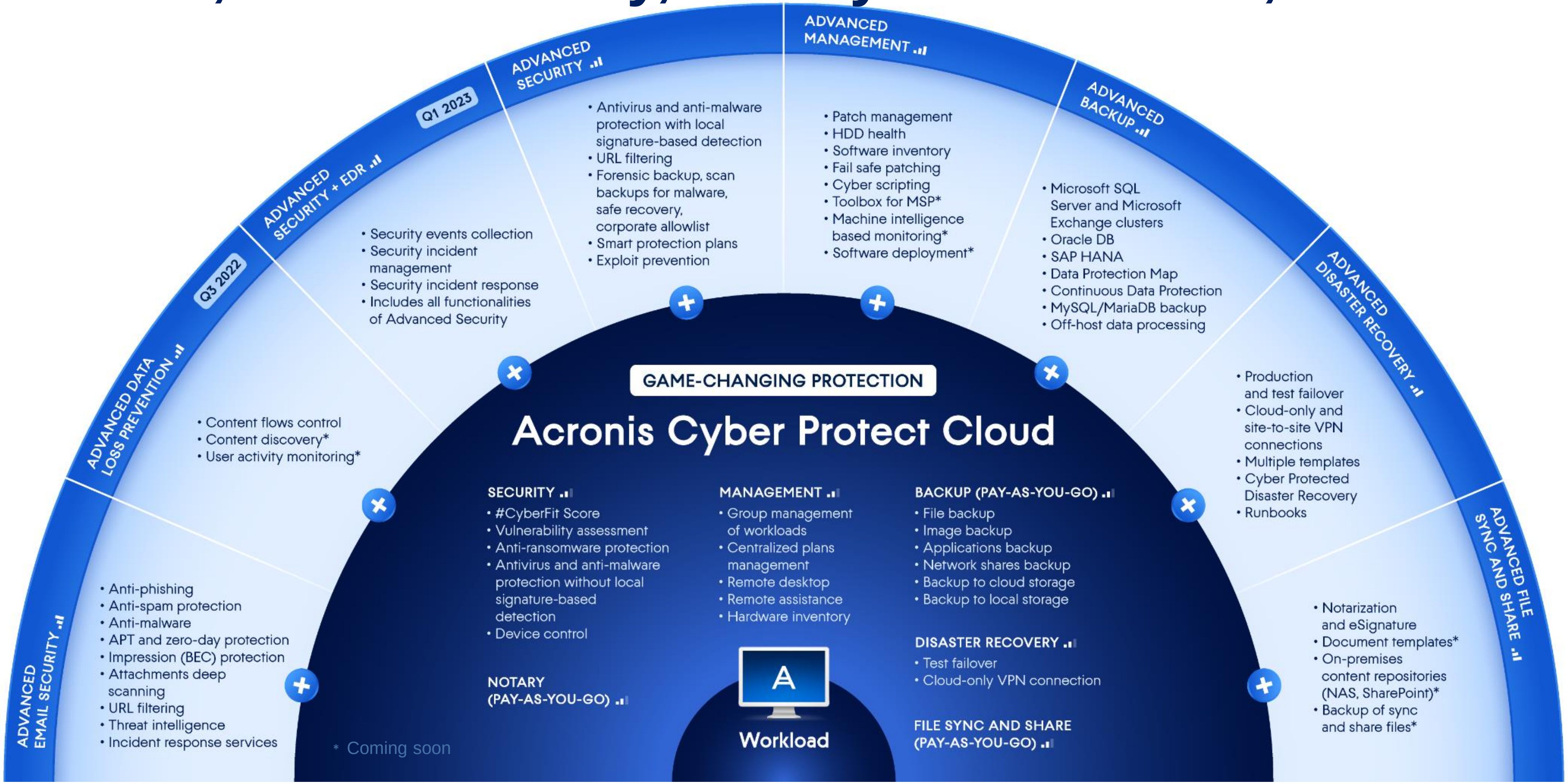
- **Help client achieve compliance with regulations** HIPAA, GDPR, PCI-DSS, etc.

Acronis

#CyberFit

Advanced DLP: Overview

Advanced packs: Security, Management, Backup, DR, Email Security, File Sync and Share, DLP



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

Q3 2022

ADVANCED DATA LOSS PREVENTION

- Content flows control
- Content discovery*
- User activity monitoring*

ADVANCED SECURITY + EDR

- Security events collection
- Security incident management
- Security incident response
- Includes all functionalities of Advanced Security

Q1 2023

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 MANAGEMENT

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

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

ADVANCED DISASTER RECOVERY

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

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

SECURITY

- #CyberFit Score
- Vulnerability assessment
- Anti-ransomware protection
- Antivirus and anti-malware protection without local signature-based detection
- Device control

NOTARY (PAY-AS-YOU-GO)

MANAGEMENT

- Group management of workloads
- Centralized plans management
- Remote desktop
- Remote assistance
- Hardware inventory

BACKUP (PAY-AS-YOU-GO)

- File backup
- Image backup
- Applications backup
- Network shares backup
- Backup to cloud storage
- Backup to local storage

DISASTER RECOVERY

- Test failover
- Cloud-only VPN connection

FILE SYNC AND SHARE (PAY-AS-YOU-GO)

Workload

* Coming soon

Advanced DLP

Prevent leakage of clients’ sensitive data

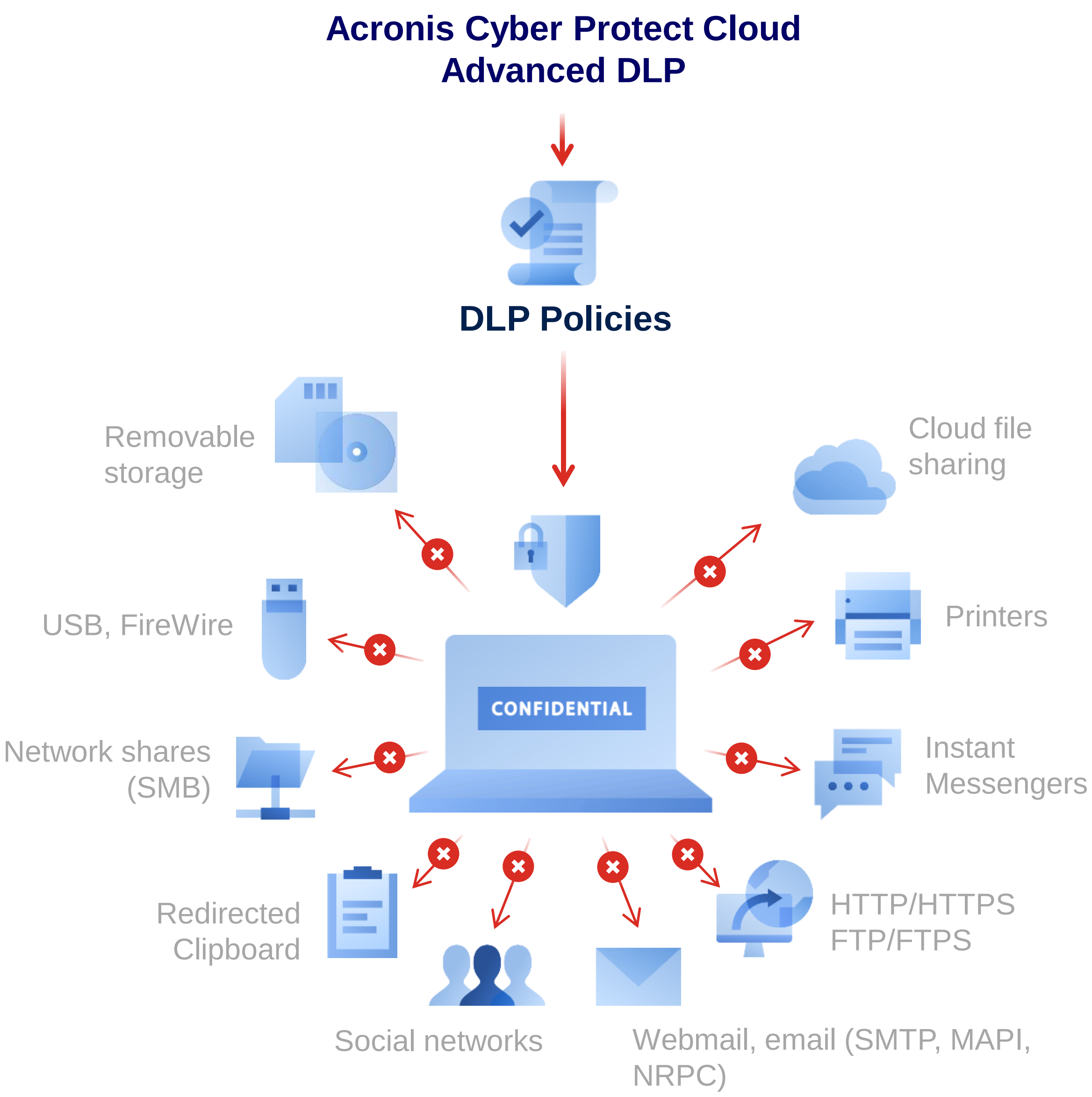
Analyze the content and context of data transfers via peripheral devices and network communications and enforce preventive controls, pre-defined in policies.

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.



Acronis Cyber Protect Cloud Advanced DLP

DLP Policies

CONFIDENTIAL

Removable storage

Cloud file sharing

USB, FireWire

Printers

Network shares (SMB)

Instant Messengers

Redirected Clipboard

HTTP/HTTPS FTP/FTPS

Social networks

Webmail, email (SMTP, MAPI, NRPC)

DLP control types

For thorough control over data flows

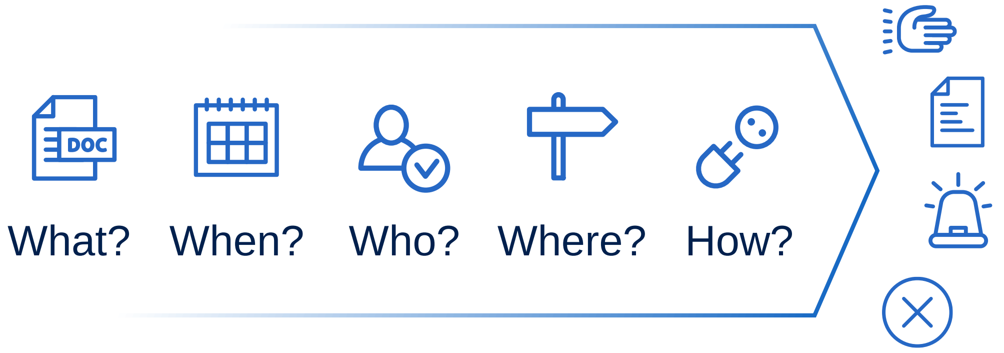
Context-aware controls – Control data access and transfer operations based on the operation's context (environmental factors) using attributes such as involved users, used channels, accessed/transferred data type, flow direction, date and time, etc.

- **Example:** Allow copying data (what) by users (who) to encrypted USB devices (where) and block copying data to unencrypted USB devices.

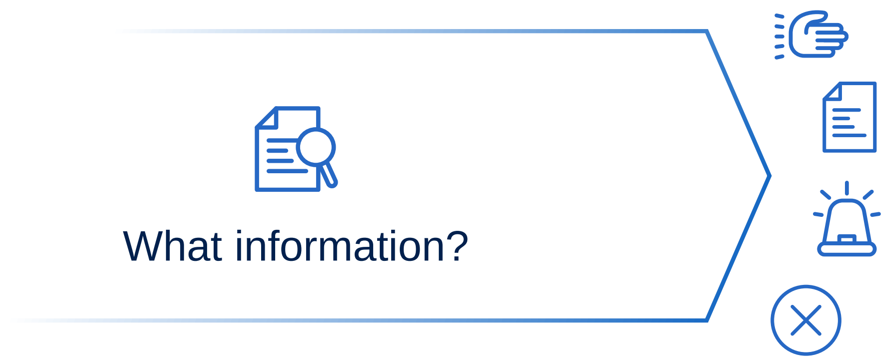
Content-aware controls – Deeper control over data access and transfer operations based on the actual information (content) being accessed or transferred.

- **Example:** Documents containing HIPAA-related information (what information) are prohibited to be copied to any USB device.

Context-aware controls

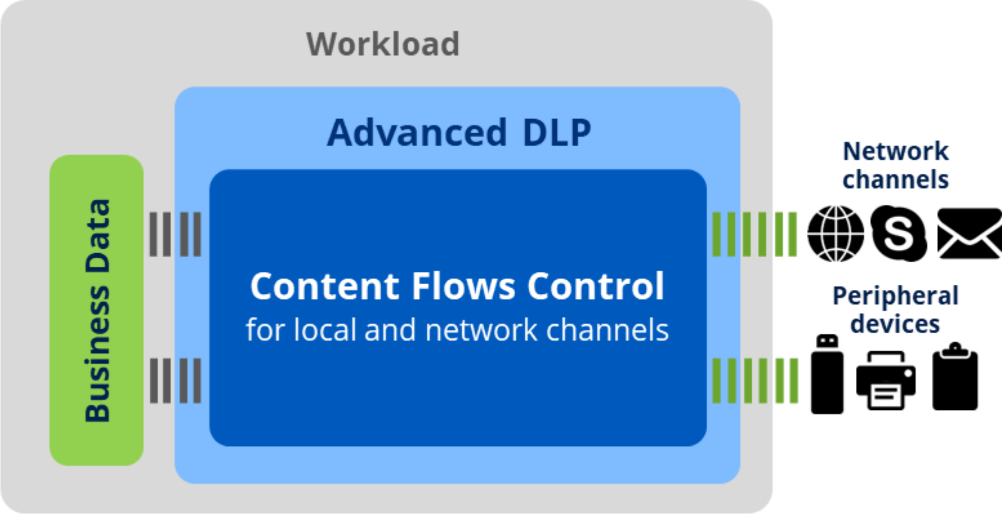


Content-aware controls



Advanced DLP – security functions

Content-aware controls over most risky channels to protect most vulnerable sensitive data

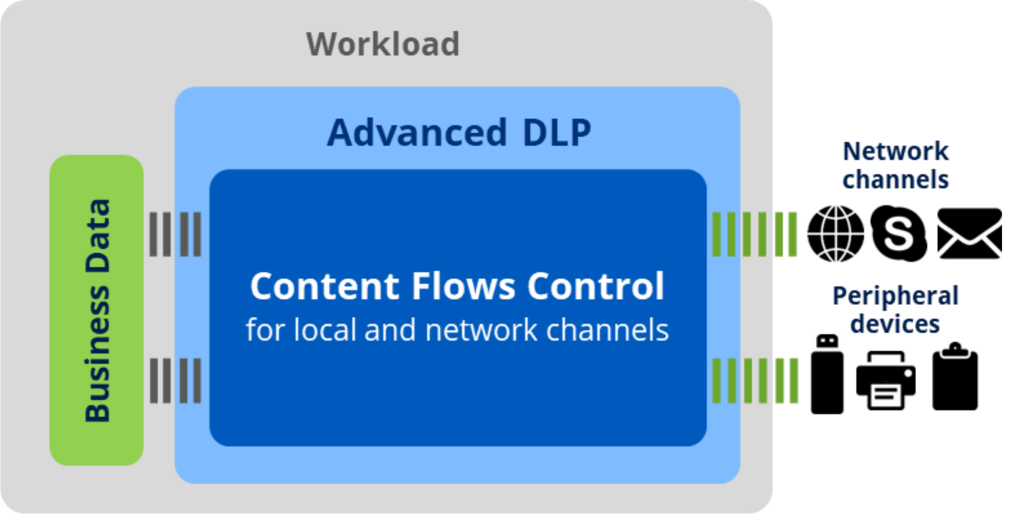


Content inspection and filtering

- **Local channels**
  - **Removable storage, printers, redirected mapped drives, redirected clipboard**
- **Network communications**
  - **Emails** – SMTP, Microsoft Outlook (MAPI), IBM Notes
  - **Instant messaging** – Skype, Viber, Zoom, Jabber, ICQ, IRC
  - **Webmail services** – ABV Mail, AOL Mail, freenet.de, Gmail, GMX Mail, iCloud, Outlook.com, Mail.ru, Outlook Web App (OWA), NAVER, Rambler Mail, T-online.de, Web.de, Yahoo! Mail, Yandex Mail, Zimbra
  - **File sharing services** – 4shared, Amazon S3, AnonFile, Box, Cloud Mail.ru, dmca.gripe, Dropbox, DropMeFiles, Easyupload.io, Files.fm, freenet.de, GitHub file sharing service, GMX File Storage, Gofile.io, Google Docs / Google Drive, iCloud, iDrive, MEGA, MagentaCLOUD, MediaFire, OneDrive, Sendspace, transfer.sh, TransFiles.ru, Uploadfiles.io, Web.de, WeTransfer, Yandex.Disk
  - **Social networks** – Disqus, Facebook, Instagram, LinkedIn, LiveInternet.ru, LiveJournal, MeinVZ.de, Odnoklassniki.ru, Pinterest, StudiVZ.de, Tumblr, Twitter, Vkontakte, XING.com
  - **Protocols** – Local network file sharing (SMB), web access (HTTP/HTTPS), file transfers (FTP/FTPS)

Advanced DLP – security functions (cont.)

Content-aware controls over most risky channels to protect most vulnerable sensitive data



Content inspection and filtering

- Structured data detectors: keywords, regular expressions
- Text parsers for 100+ file, 40+ archive, 5 print formats
- Text detection in data of unidentified type and binaries
- Nested archives inspection

Agent-resident optical character recognition (OCR)

- Works for 30+ languages without sending images to OCR servers

Pre-built data classifiers

- Personally identifiable information (PII), protected health information (PHI), payment card data (PCI DSS), “Marked as “Confidential”

Policy-based logging and real-time alerting, interactive on-screen notifications to end users

Integration with Device Control

- Access controls for peripheral devices seamlessly complement advanced content-aware data loss prevention

Protected workload types

- Physical and virtual machines running Windows 7 SP1+ and Windows Server 2008 R2+

DLP for clients’ 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, postal address, SSN, passport number, driving 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

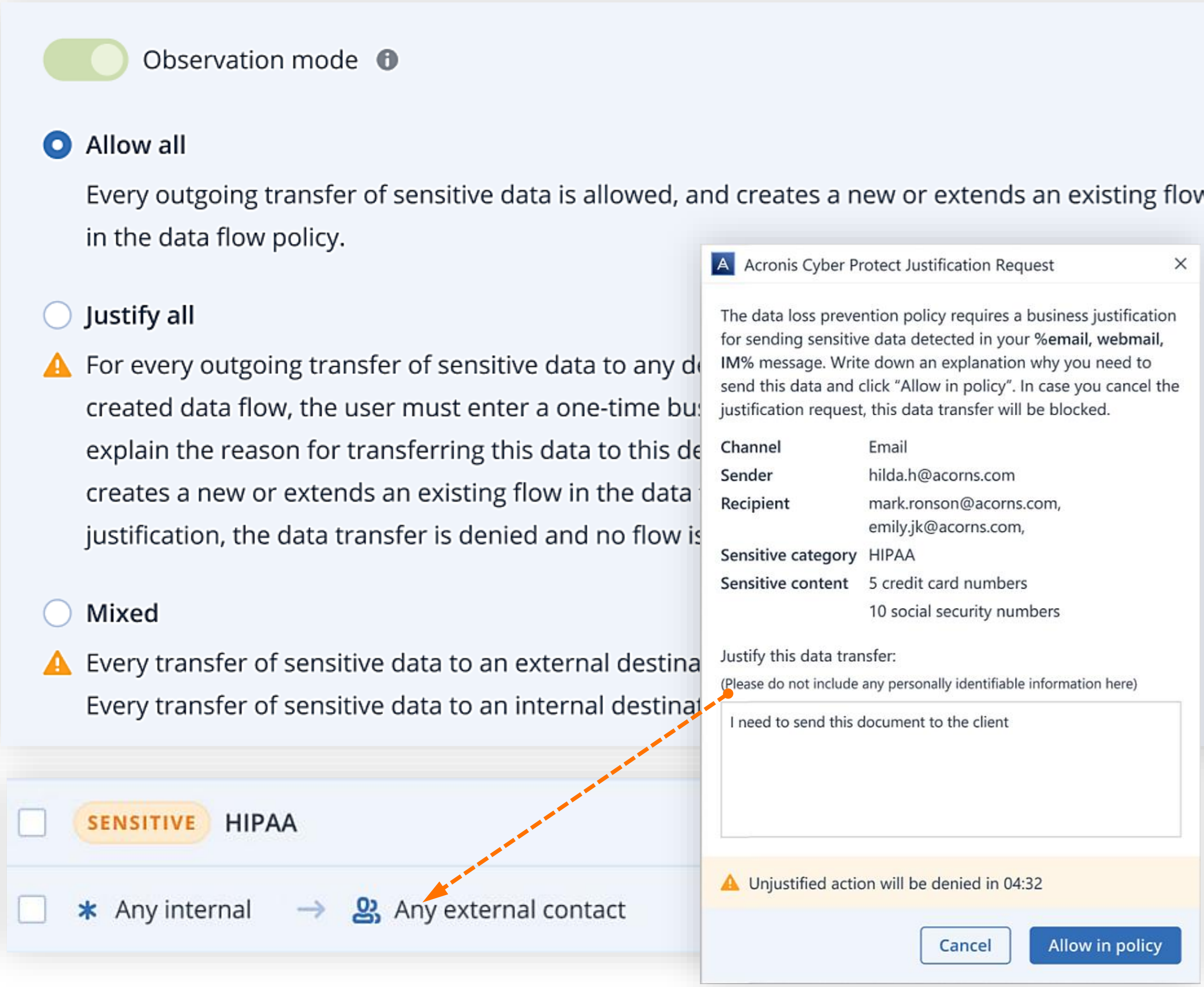
Prevent uploads of sensitive business documents with the “Confidential” watermark to employees’ private storage at file sharing services

Automatic, client-specific DLP policy generation

Simplified service provisioning and initial DLP policy configuration

Observation mode

- Automate baseline DLP policy set up - Monitor all sensitive data flows across clients' environment and create new rules in the DLP policy automatically
- Generate business - specific policies automatically without the need to spent time learning clients' business specifics
  - Allow only those data flows necessary to perform the business activities detected in the Observation mode.
- Reduce chances of errors, leading to business disruptions and increase DLP policies accuracy
  - Optional end-user justification during baseline DLP policy generation
  - Effortlessly validate every data flow with clients 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 d created data flow, the user must enter a one-time bu explain the reason for transferring this data to this de creates a new or extends an existing flow in the data justification, the data transfer is denied and no flow is

○ Mixed

⚠ Every transfer of sensitive data to an external destina Every transfer of sensitive data to an internal destina

□ 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

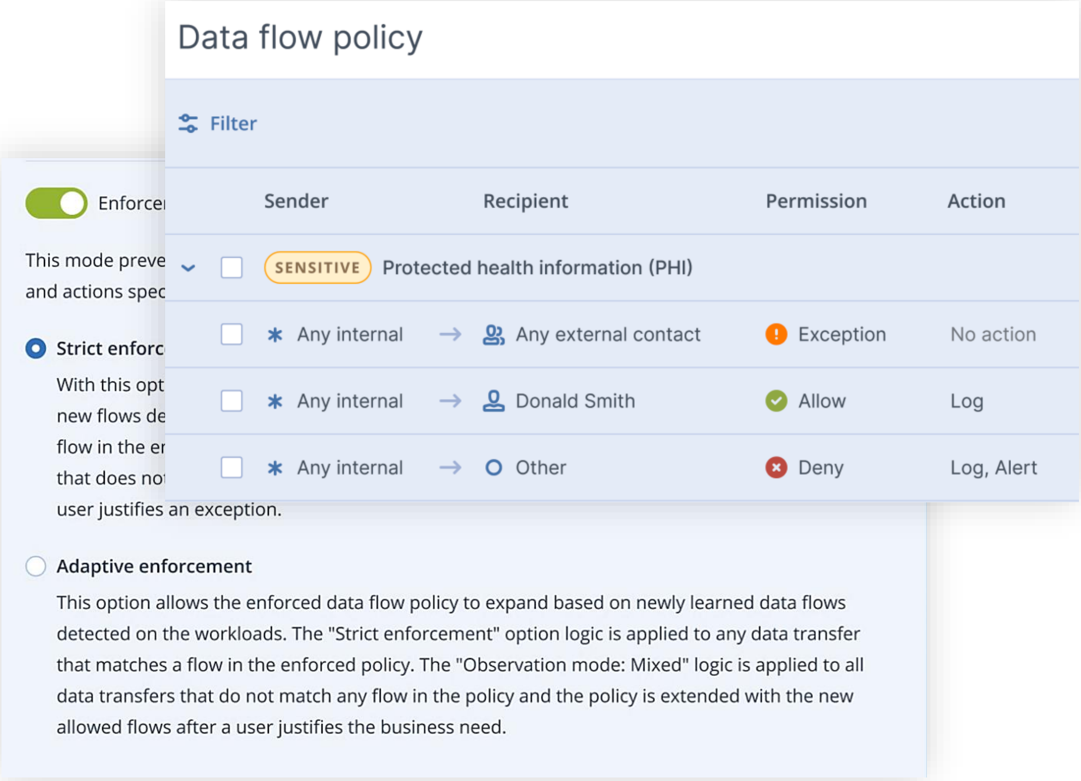
⚠ Unjustified action will be denied in 04:32

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
- Minimize work spend on policy enrichments and adjustments
- Reduce business disruptions for clients introduced by new data flows needed to operate



Enforce

This mode preve and actions spec

● Strict enforc

With this opt new flows de flow in the er that does no user justifies an exception.

○ 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

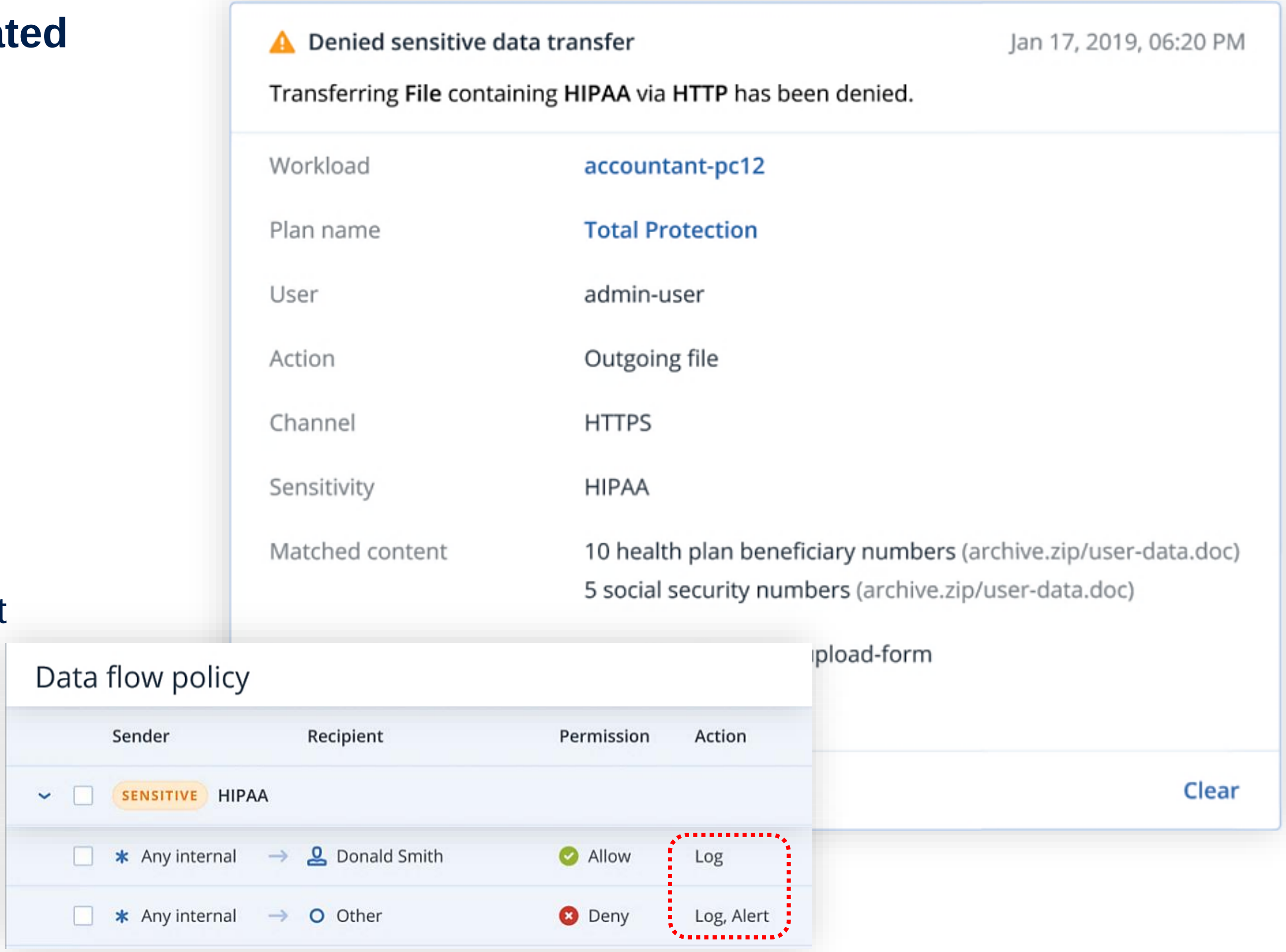
	Sender		Recipient	Permission	Action
□	SENSITIVE Protected health information (PHI)				
□	✱ Any internal	→	Any external contact	Exception	No action
□	✱ Any internal	→	Donald Smith	Allow	Log
□	✱ Any internal	→	○ Other	Deny	Log, Alert

Increase visibility with centralized logging and alerting

Simplify DLP service operations, policy maintenance, IT security audits, incident investigations

Audit logs and alerts on security events can be generated selectively for each DLP policy rule

- Store logs, protected against tampering
  - Cloud-native, secure, always available central log storage with automatic log collection and secure delivery
  - Local log storage on workloads – proprietary protected log, Windows Event Log
- Set audit log retention rules
- Increase visibility over DLP events
  - Unified view for DLP events with fast search and filtering
  - Real-time alerts and email notifications to administrators about security events
- Strengthen end-users' DLP awareness with on-screen notification



⚠ Denied sensitive data transfer

Jan 17, 2019, 06:20 PM

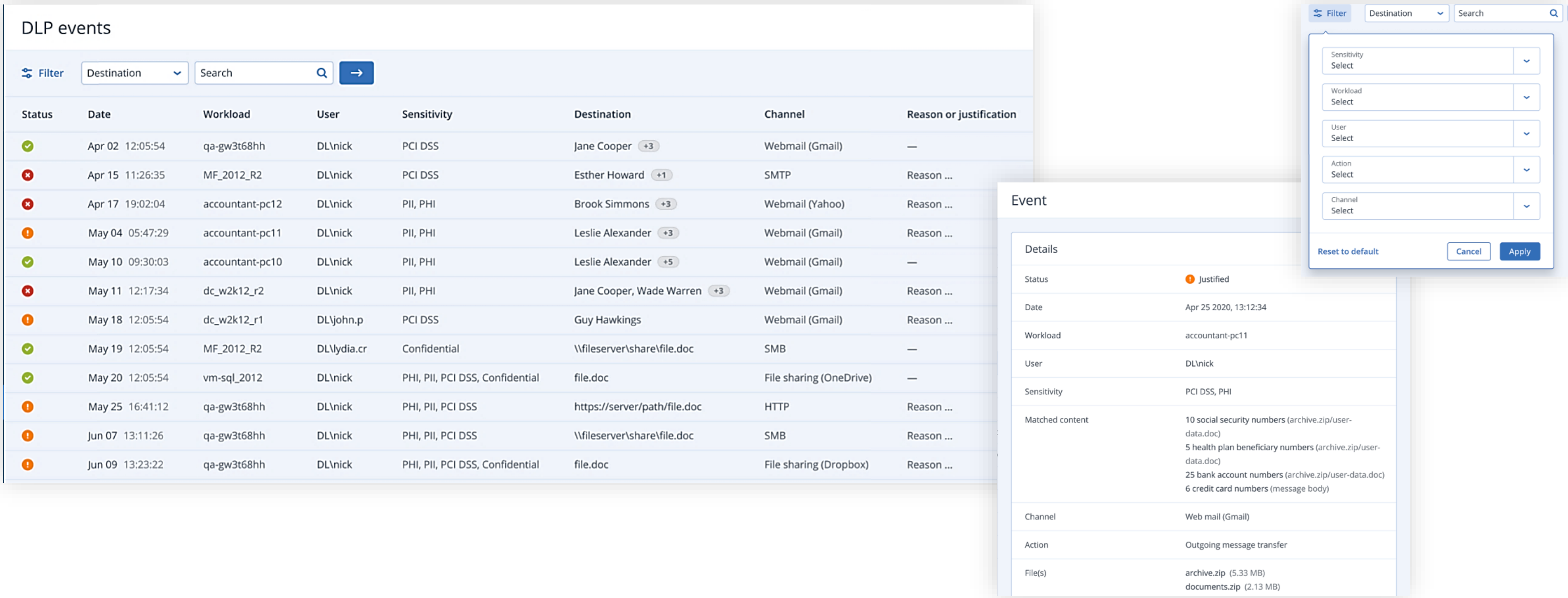
Transferring **File** containing **HIPAA** via **HTTP** has been denied.

Workload	accountant-pc12
Plan name	Total Protection
User	admin-user
Action	Outgoing file
Channel	HTTPS
Sensitivity	HIPAA
Matched content	10 health plan beneficiary numbers (archive.zip/user-data.doc) 5 social security numbers (archive.zip/user-data.doc)
	pload-form

Data flow policy

	Sender		Recipient	Permission	Action
⌄ □	SENSITIVE HIPAA				
□	✱ Any internal	→	Donald Smith	✓ Allow	Log
□	✱ Any internal	→	○ Other	✕ Deny	Log, Alert

Fast searching and filtering of DLP events



DLP events

Status	Date	Workload	User	Sensitivity	Destination	Channel	Reason or justification
✓	Apr 02 12:05:54	qa-gw3t68hh	DL\nick	PCI DSS	Jane Cooper +3	Webmail (Gmail)	—
✗	Apr 15 11:26:35	MF_2012_R2	DL\nick	PCI DSS	Esther Howard +1	SMTP	Reason ...
✗	Apr 17 19:02:04	accountant-pc12	DL\nick	PII, PHI	Brook Simmons +3	Webmail (Yahoo)	Reason ...
!	May 04 05:47:29	accountant-pc11	DL\nick	PII, PHI	Leslie Alexander +3	Webmail (Gmail)	Reason ...
✓	May 10 09:30:03	accountant-pc10	DL\nick	PII, PHI	Leslie Alexander +5	Webmail (Gmail)	—
✗	May 11 12:17:34	dc_w2k12_r2	DL\nick	PII, PHI	Jane Cooper, Wade Warren +3	Webmail (Gmail)	Reason ...
!	May 18 12:05:54	dc_w2k12_r1	DL\john.p	PCI DSS	Guy Hawkings	Webmail (Gmail)	Reason ...
✓	May 19 12:05:54	MF_2012_R2	DL\lydia.cr	Confidential	\\fileserver\share\file.doc	SMB	—
✓	May 20 12:05:54	vm-sql_2012	DL\nick	PHI, PII, PCI DSS, Confidential	file.doc	File sharing (OneDrive)	—
!	May 25 16:41:12	qa-gw3t68hh	DL\nick	PHI, PII, PCI DSS	https://server/path/file.doc	HTTP	Reason ...
!	Jun 07 13:11:26	qa-gw3t68hh	DL\nick	PHI, PII, PCI DSS	\\fileserver\share\file.doc	SMB	Reason ...
!	Jun 09 13:23:22	qa-gw3t68hh	DL\nick	PHI, PII, PCI DSS, Confidential	file.doc	File sharing (Dropbox)	Reason ...

Event

Details

Status	! Justified
Date	Apr 25 2020, 13:12:34
Workload	accountant-pc11
User	DL\nick
Sensitivity	PCI DSS, PHI
Matched content	10 social security numbers (archive.zip/user-data.doc) 5 health plan beneficiary numbers (archive.zip/user-data.doc) 25 bank account numbers (archive.zip/user-data.doc) 6 credit card numbers (message body)
Channel	Web mail (Gmail)
Action	Outgoing message transfer
File(s)	archive.zip (5.33 MB) documents.zip (2.13 MB)

Sensitivity
Select

Workload
Select

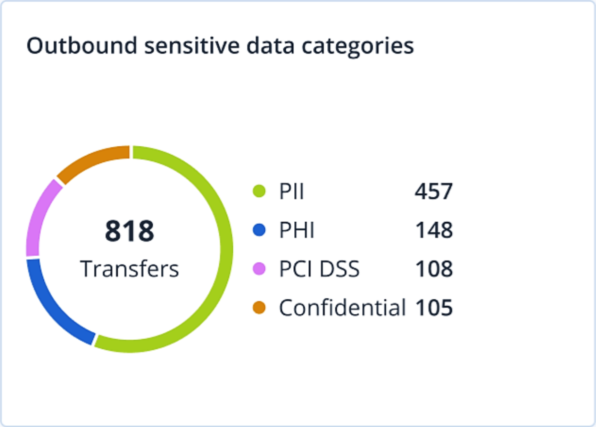
User
Select

Action
Select

Channel
Select

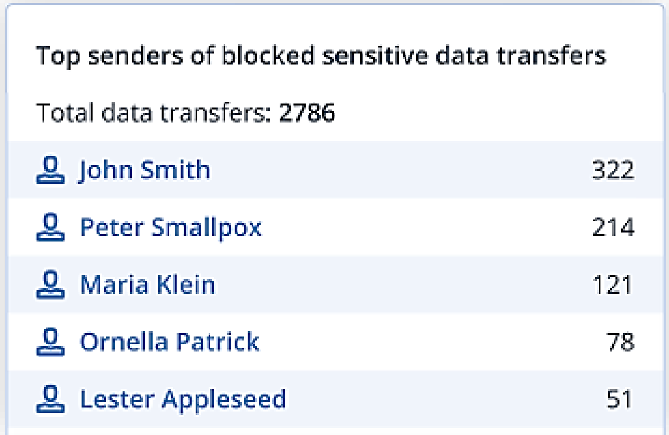
Demonstrate your services' value to clients

Information-rich widgets ease compliance reporting and provide deeper visibility into DLP performance



Outbound sensitive data categories

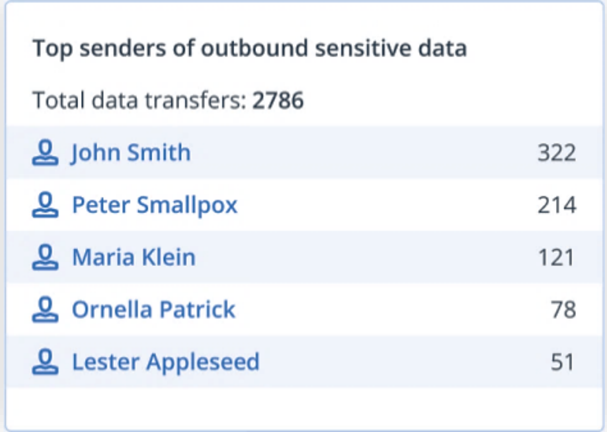
● PII	457
● PHI	148
● PCI DSS	108
● Confidential	105



Top senders of blocked sensitive data transfers

Total data transfers: 2786

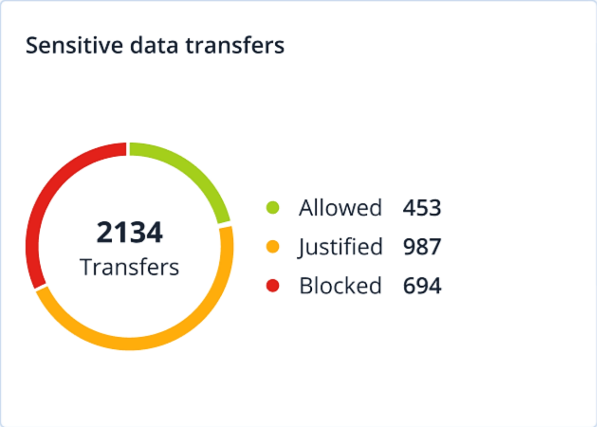
John Smith	322
Peter Smallpox	214
Maria Klein	121
Ornella Patrick	78
Lester Appleseed	51



Top senders of outbound sensitive data

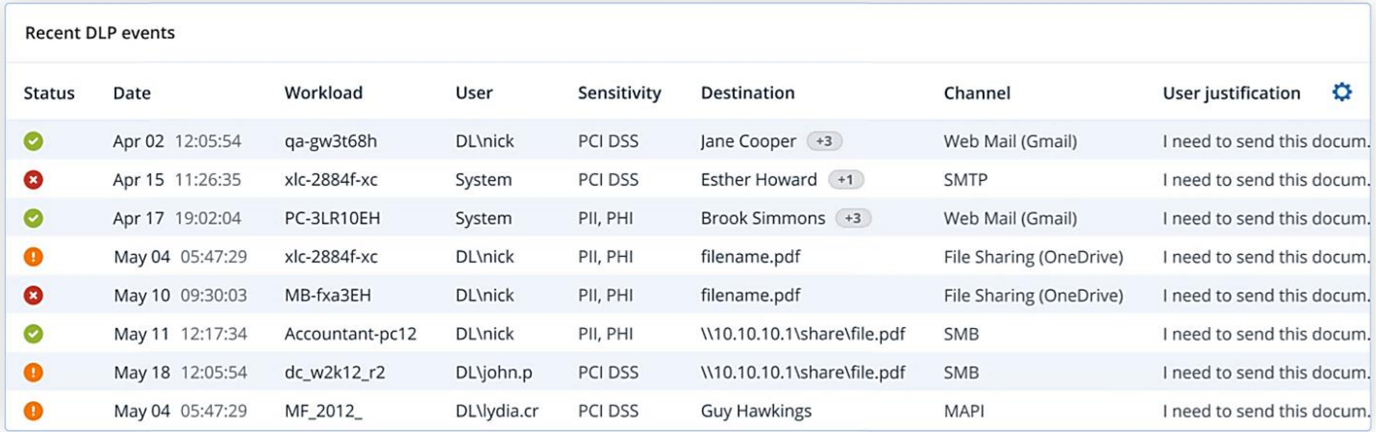
Total data transfers: 2786

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



Sensitive data transfers

● 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

Competitive positioning

How Advanced DLP differs from competition?

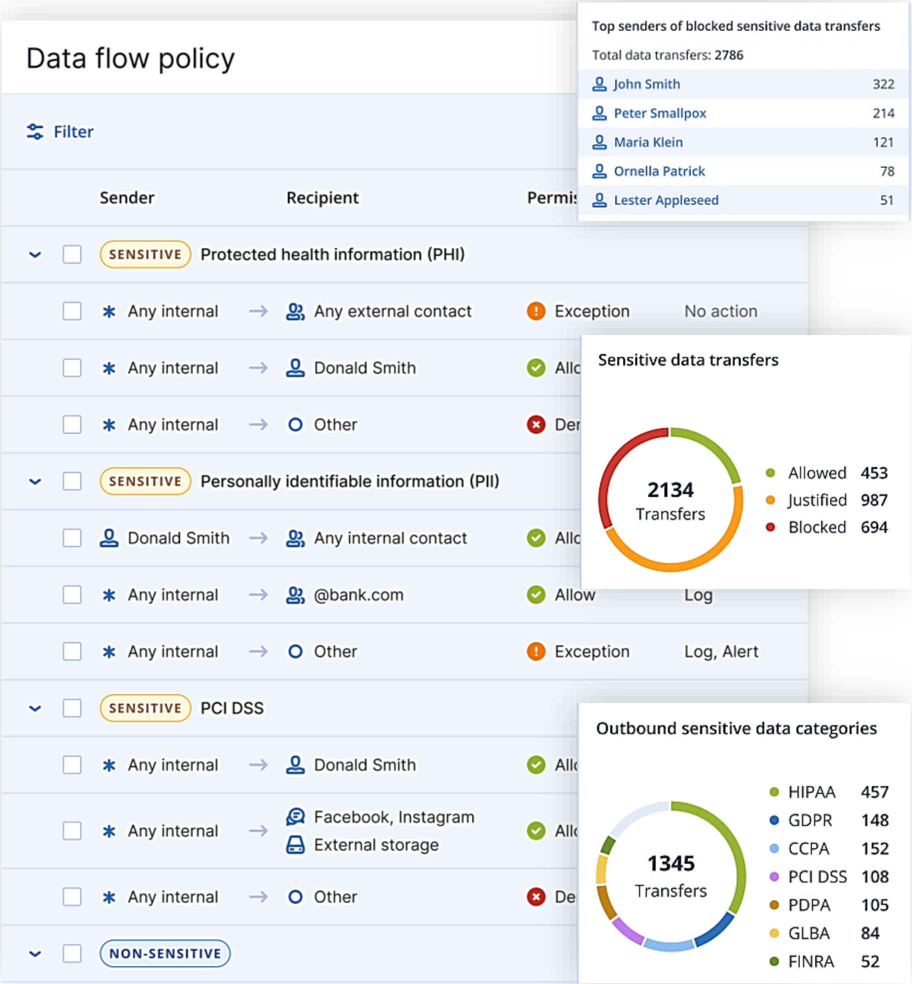
Automates DLP policy generation that learns from end users

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	Permis	
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	Allo	
	Any internal	→	Facebook, Instagram External storage	Allo	
	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

Additional competitive advantages to consider

Control data flows across more channels than 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
- File sharing, web access, and file transfer protocols

Comprehensive DLP controls to differentiate your service

- Control data transfers to social media, webmail and file-sharing services **across any browser**
- Detect and prevent leakage of **sensitive data in a graphical form,** including from remote and offline computers
- Inspect the **content** of outgoing instant messages
- Control data flows on **remote and offline computers**

Centralized cyber protection with a single console

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.

Acronis

#CyberFit

Licensing

Overview

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

Acronis

#CyberFit

How the DLP service is provisioned to clients?

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
Cyber Foundation

Building a more knowledgeable future

#CyberFit

Create, spread and protect knowledge with us!

- Building new schools
- Providing educational programs
- Publishing books

www.acronis.org