Acronis

#CyberFit

Advanced DLP security functions

Functional specifications document

Content inspection and filtering (Windows)

Controlled local channels (“data in use” DLP)

Feature	Feature support/ parameters	Feature description/notes
Removable storage	Files	Content detection and flow control of data (files) transferred to removable storage devices
Encrypted removable storage	Files	Content detection and flow control of data (files) transferred to removable storage devices encrypted by BitLocker To Go
Printers	Print jobs	Content detection and flow control of data transferred to physical printers: application and printer independent inspection of **EMF, PDF, PostScript, PCL5, PCL6 (PCL XL)** print jobs
Redirected mapped drives	Files	Content detection and flow control of data (files) transferred from desktop/application/VDI sessions on host servers or workloads to mapped drives (removable, hard, optical) redirected from remote BYOD/terminals
Redirected clipboard	Files, text, images, audio, unidentified data	Content detection and flow control of data transferred from desktop/application/VDI sessions on host servers or workloads to redirected clipboards of remote BYOD/terminals. Types of inspected data objects: **files, textual data, images, audio, unidentified data**.

Content inspection and filtering (Windows)

Controlled network channels (“data in motion” DLP)

Feature	Feature support/ parameters	Feature description/notes
SMTP e-mails	Messages, attachments	Content detection and flow control of data in outgoing emails sent over SMTP/SMTPS from *any application*
Microsoft Outlook (MAPI)	Messages, attachments	Content detection and flow control of data in outgoing emails sent from Microsoft Outlook over MAPI
IBM Notes	Messages, attachments	Content detection and flow control of data in outgoing emails sent from IBM Notes emails over NRPC
Webmails	Messages, attachments	Content detection and flow control of data sent in webmails from *any web browser* (Gmail, Outlook.com, Outlook Web App (OWA), iCloud, Yahoo! Mail, T-online.de, AOL Mail, ABV Mail, freenet.de, GMX Mail, Mail.ru, NAVER, Rambler Mail, Web.de, Yandex Mail, Zimbra)
Instant messaging	Messages, files	Content detection and flow control of outgoing messages and files in instant messaging communications via Skype, Zoom, Jabber, Viber, ICQ (plain/SSL), IRC (plain/SSL), Mail.ru Agent (plain/SSL)
File sharing services (web-based access)	Files, web forms	Content detection and flow control of outgoing data in communications from *any web browser* with file sharing services (Google Drive, Google Docs/Slides/Sheets, OneDrive, Box, Dropbox, GitHub, GMX File Storage, Amazon S3, MEGA, WeTransfer, freenet.de, Web.de, Sendspace, MagentaCLOUD, Easyupload.io, 4shared, MediaFire, Gofile.io, iCloud, Uploadfiles.io, AnonFile, iDrive, Files.fm, DropMeFiles, transfer.sh, TransFiles.ru, Cloud Mail.ru, Yandex.Disk)
Social networks	Messages (posts), files	Content detection and flow control of data transferred from *any web browser* to social networks (Facebook, LinkedIn, Twitter, XING.com, Disqus, Instagram, Vkontakte, Pinterest, Tumblr, LiveInternet.ru, LiveJournal, Odnoklassniki.ru)
Web access (HTTP/HTTPS)	Files, web forms	Content detection and flow control of outgoing data in generic web-based communications over HTTP/HTTPS from *any web browser*
File transfers (FTP/FTPS)	Files	Content detection and flow control of outgoing files transferred from *any application* over FTP/FTPS protocols
Local network file sharing (SMB)	Files	Content detection and flow control of outgoing files in the local network over the SMB protocol 1. Data upload from the workload to external network shares 2. Data download from a workload's shared folder by users on external workloads

Content inspection and filtering (Windows)

Controlled detection features

Feature	Feature support/ parameters	Feature description/notes
Protected content types		Types of content used for classifying data to sensitivity categories in DLP policy
Textual data	Yes	Content is associated with textual data contained in data objects
Data types	No*	Content is associated with the type of data object (e.g. a file type) * Expected in Q4'22
Metadata	No*	Content is associated with metadata of a data object (e.g. document or file properties) * Support postponed to a future update
Objects inspected for textual content		
Files	100+	Parsing textual content from 100+ file formats
Archives	40+	Parsing textual content from 40+ archive types
Print jobs	5	Parsable print job types: EMF, PDF, PostScript, PCL5, PCL6 (PCL XL)
Other textual objects	Yes	E-mail messages, instant messages, web forms, posts, comments
Images	Yes	Textual content detection in graphical files (30+ formats) and embedded images in documents, emails, instant messages, posts and other data objects
Binaries	Yes	Text detection in binary data (without data object parsing and text normalization)

Content inspection and filtering (Windows)

Controlled detection features

Feature	Feature support/ parameters	Feature description/notes
Textual content detection methods		
Keywords	Yes	Content detection based on specified keywords or phrases
Keyword morphological analysis	No*	English, French, German, Italian, Russian, Spanish, Catalan Spanish, Portuguese, Polish * Support postponed to a future update
Regular expression (regexp) patterns	Yes	Content detection based on the specified patterns of alphanumeric text described by Perl regular expressions
Document (data) fingerprinting	No*	Content detection based on document fingerprints (hashes of data fragments in the document) * Expected in 2023
Exact file matching	No*	Identification of a file's sensitivity classification based on its exact match with a source file of known sensitivity classification. Files match if their checksums are identical. * Expected in 2023
Data type detection methods		
File type detection	No*	Detection of a file's true file type based on its binary signatures rather than just its extension * Expected in Q4'22
Clipboard data type detection	Yes*	Detection of types of data copied via the Windows clipboard and redirected clipboards (files, textual data, images, audio, unidentified) * Supported for enabling content inspection of data transferred from the workload via redirected clipboards

Content inspection and filtering (Windows)

Controlled detection features

Feature	Feature support/ parameters	Feature description/notes
Detectable metadata		
Document (file) properties	No*	Recognition of file properties (i.e. size, name, header information, date modified, etc.) * Will be considered for a future update if requested by customers
Labels assigned to data objects by 3rd-party data classification solutions	No*	Identification of a data object's sensitivity classification based on its label assigned by Boldon James Classifier * Will be considered for a future update if requested by customers
Composite content detection	Yes*	Content detection based on a combination of various content detection methods * Keywords and regexp patterns are currently used for composite content detection in prebuilt data classifiers. Once other content detection methods are supported in Advanced DLP, they will also be used in composite content detection.

Content inspection and filtering (Windows)

Data classification

Feature	Feature support/ parameters	Feature description/notes
Prebuilt sensitive data classifiers	Yes (4)	Prebuilt composite data classifiers allow preventing exfiltration of sensitive data of the most essential classification categories: PHI, PII, PCI DSS, "Marked as Confidential"
Custom sensitive data classifiers		Allow customers to create data classifiers for classifying data objects to a customer-specific sensitive category (e.g. IP, employee's PII, patient's PHI, etc.)
Custom structured data classifiers	No*	Custom data classifiers based on structured data detection methods (file types, keywords, regexp patterns) * File type based custom data classifiers expected in Q4'22 * Keyword and regexp pattern-based custom classifiers expected in Q4'23
Trainable custom unstructured data classifiers	No*	Custom data classifiers based on a data fingerprinting method of unstructured data detection can be created by pointing at examples of documents, files, and other data objects of known classification categories specific to the customer * Expected in H2'23
Composite custom data classifiers	No*	Composite custom data classifier is created by logically combining (Boolean expression) one or more prebuilt or custom textual content detectors, file type detectors, metadata detectors, and data classifiers * Expected in 2023 (except metadata detectors, which may be supported in a future update)

Content inspection and filtering (Windows)

Data classification

Feature	Feature support/ parameters	Feature description/notes
Content detectors		A logical construct specifying data inspection conditions and parameters for detecting the presence of a particular content in the inspected data object
Prebuilt file type detectors	No*	Prebuilt content detectors based on file types * Expected in Q4'22
Prebuilt keyword-based content detectors (keyword dictionaries)	No*	Prebuilt structured textual content detectors based on industry and country specific keyword dictionaries * Expected in Q2'23
Prebuilt regexp pattern-based content detectors	No*	Prebuilt structured textual content detectors based on industry and country specific regexp patterns * Expected in Q2'23
Custom file type detectors	No*	Allows customers to create their own file type detectors from scratch or by using duplicates of prebuilt file type detectors as templates * Expected in Q4'22
Custom keyword-based content detectors (keyword dictionaries)	No*	Allows customers to create their own keyword-based content detectors from scratch or by using duplicates of prebuilt keyword-based content detectors as templates * Expected in Q2'23
Custom metadata detectors	No*	Allows customers to create metadata detectors * Will be considered for a future update if requested by customers

Content inspection and filtering (Windows)

Content inspection enablement features

Feature	Feature support/ parameters	Feature description/notes
Agent-resident optical character recognition (OCR)	31 languages 30+ graphical file formats	Textual content detection in graphical files (30+ formats) and embedded images in documents, emails, instant messages, posts and other data objects (Arabic, Bulgarian, Catalan, Chinese - Simplified, Chinese - Traditional, Croatian, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Hungarian, Indonesian, Italian, Japanese, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Slovak, Slovenian, Spanish, Swedish, Turkish)
Nested archives inspection	Yes	Ability to inspect the content of files in nested archives (e.g. a file in a Zip archive inside a RAR archive)
Password-protected data transfer prevention	Yes	Ability to block the transfer of password-protected data to prevent potential data leak (as the content of this data cannot be inspected)
Data transfer prevention on inspection errors	Yes	Ability to block the data transfer if an error occurs during its content inspection

Contextual controls (Windows)

Local contextual control features

Feature	Feature support/ parameters	Feature description/notes
Allowlist for device types	Yes	*Protection plan-wide control:* data transfers to the allowlisted types of controlled peripheral devices are allowed regardless of their data sensitivity and the enforced DLP policy (removable storage, mapped drives, redirected clipboard, printers)
Process exclusions	Yes	Allowlisted processes are excluded from access controls set for clipboards (local and redirected), screenshot capture, printer, and mobile devices.
Allowlist for applications	Yes	*Protection plan-wide control*: data transfers performed by the allowlisted applications are allowed regardless of their data sensitivity and the enforced DLP policy
Data transfer prevention on inspection errors	Yes	Ability to block the data transfer if an error occurs during its content inspection

Network contextual control features

Allowlist for network communications	Yes	*Protection plan-level control:* data transfers over the allowlisted types of network channels (e.g. webmails, SMTP emails, file sharing services, social networks, SMB file shares, etc.) are allowed regardless of data sensitivity and the enforced DLP policy for all workloads under this plan
Allowlist for remote hosts	Yes	*Protection plan-level control*: data transfers to the allowlisted remote hosts (FQDN, IP address) are allowed regardless of their data sensitivity and the enforced DLP policy for all workloads under this plan

Enforcement actions

Actions for data transfer controls in local channels and network communications

Feature	Feature support/ parameters	Feature description/notes
Allow	Yes	A rule with this permission allows any data transfer matching this rule
Deny	Yes	A rule with this permission blocks any data transfer matching this rule
Detect	No*	A rule with this permission detects and logs any data transfer matching this rule * Expected to be supported in Q3'23 for WhatsApp and Telegram. As policy rules in Advanced DLP are channel-independent, the "Detect" permission will not be configurable and will not be displayed in UI. It will be applied by default for data transfers in those controlled channels where Advanced DLP supports only content detection but cannot block data transfers.
Shadow	No*	A rule with this action creates a shadow copy of data carried on in a data transfer matching this rule to the DLP shadow log * Will be considered for a future update of Advanced DLP in Cyber Protect Cloud if requested by customers. * Considered for support in Advanced DLP as a component of Cyber Protect on-prem.
Exception	Yes	A rule with this permission blocks any data transfer matching this rule with the option for user to override the block by requesting an exception
Log	Yes	An event record is stored in the audit log when a data transfer matches a rule with this action set on
Alert	Yes	An alert is generated and sent when a data transfer matches a rule with this action set on
Notify user on data transfer denial	Yes	An on-screen notification is displayed to the user whose data transfer has matched a rule with this action set on

Logging

Policy-based logging

Feature	Feature support/ parameters	Feature description/notes
Policy-based logging	Yes	Audit logs are generated selectively on per policy rule basis

Collected log types

Audit log	Yes	A log of events generated by managed DLP agents on end user-initiated operations controlled by DLP policies
Shadow log	No*	A log containing shadow copies of data carried on in data transfers matching policy rules that have the "Shadow" action set on. * Will be considered for a future update of Advanced DLP in Cyber Protect Cloud if requested by customers. * Considered for support in Advanced DLP as a component of Cyber Protect on-prem.
Agent (monitoring) log	No*	A log of all types of DLP agent service-specific events on managed DLP agents (e.g. agent start/stop, policy changes, local storage issues, etc.) Management of administrative roles and functions in DLP Logging Subsystem * Will be supported in a future update
Administrative log	No*	A log of actions performed by users with administrative roles to manage Advanced DLP * Will be supported in a future update

Logging

Types of logged data transfer-related events

Feature	Feature support/ parameters	Feature description/notes
Allow	Yes	An event when a data transfer matches a policy rule with the Allow permission
Exception	Yes	An event of a block override (exception) request submitted by end user in the enforcement mode
Justify	Yes	An event of a sensitive data flow justification submitted by an end user in the observation mode
Deny	Yes	An event when a data transfer matches a policy rule with the Deny permission
Detect	No*	An event when a policy rule with the Deny or Exception permission is triggered by a data transfer in a channel where Advanced DLP can only detect data content but cannot prevent data transfers. * Expected to be supported in 2023 for WhatsApp and Telegram

Workload log storage

Protected local log	Yes	Protected log storage on the workload
Windows Event log	Yes	Windows Event Log is used for logging start/stop events and severe errors in DLP agent operations for their remote troubleshooting with Windows Event Viewer

Logging

Central log storage

Feature	Feature support/ parameters	Feature description/notes
Cloud-based central log storage	Yes	Central log storage is supported for Advanced DLP events
Central audit log storage type	Yes	Central log storage is supported for Advanced DLP events

Centralized log collection

Automatic log collection to the central log database	Yes	Centralized log collection is supported for Advanced DLP events
Secure log delivery to the central log database	Yes	Centralized log collection is supported for Advanced DLP events

Alerting and notifications

Policy-based alerting

Feature	Feature support/ parameters	Feature description/notes
Policy-based alerting	Yes	Real-time alerts on security events are generated selectively on per policy rule basis

Administrative alerts and notifications

Alert sources		
DLP agents	Yes	
Alert destinations		
Cyber Protect service console	Yes	
External log management and SIEM systems	No*	* Could be considered for a future update if requested by customers
E-mail notification sources		
DLP backend service	Yes	
E-mail notification destinations		
Administrators	Yes	

Alerting and notifications

Administrative alerts and notifications

Feature	Feature support/ parameters	Feature description/notes
Alert types		
DLP service usage related	Yes	
Security event related	Yes	
Alert and notification delivery methods		
Proprietary	Yes	Standard alert delivery protocols are used (SNMP, SYSLOG)
SMTP	Yes	To administrators
SNMP (with MIB)	No*	To external log management and SIEM systems * Could be considered for a future update if requested by customers
SYSLOG	No*	To external log management and SIEM systems * Could be considered for a future update if requested by customers

Alerting and notifications

End-user notifications

Feature	Feature support/ parameters	Feature description/notes
Real-time interactive on-screen user notifications	Yes	Real-time interactive notifications appear on the computer screen to inform the end user on DLP actions impacting their business communications and getting their real-time response as necessary
Notification types		
Justification request	Yes	In the observation mode, a user initiated a previously unobserved sensitive data transfer is requested to provide a one-time business justification for allowing this and all similar subsequent data transfers by an automatically generated new or enriched existing policy rule
Exception request	Yes	A user initiated a data transfer blocked by a rule with the "Exception" permission, can override the block by requesting a one-time exception and explaining its business reason in the on-screen block notification window
Transfer denial notification	Yes	A user initiated a data transfer blocked by a rule with the "Deny" permission is real-time notified on the denial and its reason by a pop-up on-screen denial notification

Cyber Protect Agent self-protection, supported platforms

Cyber Protect Agent self-protection

Feature	Feature support/ parameters	Feature description/notes
Protection from regular end-users	Yes	
Protection from local system administrators	No	Note: password protection of Cyber Protect Agent uninstallation does not prevent local system administrators from rebooting the computer in Safe mode and removing Agent even if the password is set.

Supported platforms

Agent for DLP		
Windows	Yes	Microsoft Windows 7 Service Pack 1 and later Microsoft Windows Server 2008 R2 and later
Mac	No*	macOS 10.15 (Catalina) and later macOS 11.2.3 (Big Sur) and later * Support of macOS by Advanced DLP is expected in a future update in 2023

Management architecture

Feature	Feature support/ parameters	Feature description/notes
Deployment type	Cloud-based	
Multi-tenancy support	Yes	Support of independent management (DLP policies, settings, log collection, etc.) for different customer tenants by different partner tenants from a single management platform
Hierarchical management	Yes	Support of delegation and revocation of exclusive rights to manage a DLP management domain (company, unit, group) to and from an administrative user performed by an administrator of the parent DLP management domain
Integration into a cyber protection management platform	Yes	*Cyber Protect Cloud*
Remote management transport protocols	HTTP*	By using HTTP according to REST APIs principles, Advanced DLP is optimized for managing DLP agents and collecting logs over the Internet

DLP policy management

DLP policy management

Feature	Feature support/ parameters	Feature description/notes
Policy export, import and backup	No*	Ability to export, import, and backup DLP policy as a data object (e.g. a configuration file). * Value to be clarified
Policy version control	No*	Ability to review older policy versions, changes made and comments to these changes * Will be supported in a future update

Management methods

Manual policy creation and editing	Yes	Administrators can manually create and edit data flow policy rules
Automatic baseline policy creation	Yes	With the "Allow all" option chosen in the observation mode, Advanced DLP learns and analyzes all transfers of sensitive data from protected computers detected by DLP agents in the observation period and uses this knowledge to automatically create the baseline DLP policy corresponding to the business processes of this organization
Automated user-assisted baseline policy creation	Yes	With the "Mixed" or "Justify all" option chosen in the observation mode, Advanced DLP learns, if necessary with user assistance, and analyzes all transfers of sensitive data from protected computers detected by DLP agents in the observation period and uses this knowledge to automatically create the baseline DLP policy corresponding to the business processes of the organization
Automated user-assisted policy extension	Yes	In the adaptive enforcement mode, Advanced DLP learns, if necessary with user assistance, previously unobserved sensitive data flows from protected computers that do not match explicit rules in the enforced DLP policy and automatically extends it with newly permissive rules for adjusting the policy to the business processes of the organization.
Block override by exception	Yes	A user initiating a data transfer blocked by a rule with the "Exception" permission can override the block by requesting a one-time exception with its business reason written in the on-screen request window

DLP policy management

Operational modes

Feature	Feature support/ parameters	Feature description/notes
Observation mode	Yes	This mode automatically creates the baseline DLP policy consistent with the business processes of the client organization
Allow all	Yes	In this option, the baseline DLP policy is created fully automatically by registering any outgoing sensitive data transfer as necessary for business processes and then creating a new or enriching existing permissive data flow policy rule to allow this and all subsequent equivalent data transfers
Justify all	Yes	In this option, the baseline DLP policy is created with end user assistance by registering any outgoing sensitive data transfer that was justified by its sender as necessary for business processes and then creating a new or enriching existing permissive data flow policy rule to allow this and all subsequent equivalent data transfers
Mixed	Yes	In this option, the "Allow all" logic of policy creation is applied to any sensitive data transfer to an internal recipient or destination, while the "Justify all" logic is applied to any sensitive data transfer to an internal recipient or destination
Enforcement mode	Yes	This mode prevents leakage of sensitive data from protected computers by applying the permissions and actions specified in the enforced DLP policy rules
Strict	Yes	This option enforces the specified DLP policy as is, without extending it, according to the following logic: 1. A data transfer matching explicit policy rules is controlled by the permission and actions set in this rule. 2. A data transfer matching no explicit policy rule is controlled by the applicable default policy rule.
Adaptive	Yes	This option enforces the specified DLP policy while automatically extending it according to the following logic: 1. A data transfer matching explicit policy rules is controlled by the permission and actions set in this rule. 2. A data transfer matching no explicit policy rule is handled according to the Mixed observation mode logic.

DLP policy management

Policy object types

Feature	Feature support/ parameters	Feature description/notes
Users	Yes	Used as senders and recipients/destinations
Removable storage	Yes	Used as recipients/destinations
Encrypted removable storage	Yes	Used as recipients/destinations
File sharing services	Yes	Used as recipients/destinations
Social networks	Yes	Used as recipients/destinations
Hosts	Yes	Used as recipients/destinations
Printers	Yes	Used as recipients/destinations
Object lists		List of objects (object IDs) used as **senders** or **recipients/destinations** in DLP policy rules
User lists	Yes	Used as senders and recipients
Non-user lists	Yes	Used as recipients/destinations
Hybrid lists	Yes	Used as recipients/destinations

DLP policy management

Policy object types

Feature	Feature support/ parameters	Feature description/notes
User groups		Groups of users used as **senders** and **recipients/destinations** in DLP policy rules
Prebuilt user groups	Yes	
Custom user groups	No*	Created by administrators or imported from directories (AD, LDAP) * Expected in Q1-2023
Non-user groups		Groups of non-user objects (e.g. peripheral devices, hosts, file sharing services, social networks, printers) used as **recipients/destinations** in DLP policy rules
Prebuilt non-user groups	Yes	
Hybrid groups		Groups that include users and non-user objects (e.g. peripheral devices, hosts, file sharing services, social networks, printers) used as **recipients/destinations** in DLP policy rules
Prebuilt hybrid groups	Yes	

DLP policy management

Policy rule categories, types, and priorities for data transfer controls in local and network channels

Feature	Feature support/ parameters	Feature description/notes
Policy rule categories		
Explicit rules	Yes	DLP policy rules created explicitly (manually or automatically) to control one or more sensitive data flows in specific observed or envisioned data transfer scenarios
Default rules	Yes	An implicit DLP policy rule enforced over any data flow that matches no explicit rule in the DLP policy. The type of default rule applied to a data transfer depends on the operational mode and its option, as well as on the data sensitivity
Explicit policy rule types		The type of policy rule corresponds to the “Permission” specified in the rule
Allow	Yes	A rule with this permission allows any data transfer matching this rule
Exception	Yes	A rule with this permission blocks any data transfer matching the rule with the option for user to override the block by requesting an exception
Deny	Yes	A rule with this permission blocks any data transfer matching this rule
Allow (prioritized)	Yes	A rule with this permission allows any data transfer matching this rule
Exception (prioritized)	Yes	A rule with this permission blocks any data transfer matching the rule with the option for user to override the block by requesting an exception

DLP policy management

Policy rule categories, types, and priorities for data transfer controls in local and network channels

Feature	Feature support/ parameters	Feature description/notes
Explicit policy rule type prioritization		Prioritized permissions (rules) allow a group policy to be applied only to a part of its members. This is achieved by creating policies with a user's rule permission prioritized over the rule permission of a group with the user's membership. The policy rule type priorities are listed in the descending order.
Exception (prioritized)	Yes	The highest priority permission
Allow (prioritized)	Yes	
Deny	Yes	
Exception	Yes	
Allow	Yes	The lowest priority permission
Default policy rule types		The type of policy rule corresponds to the “Permission” specified in the rule
Allow	Yes	A default rule with this permission allows any data transfer matching no explicit rule in the DLP policy
Deny	Yes	A default rule with this permission blocks any data transfer matching no explicit rule in the DLP policy
Exception	Yes	A default rule with this permission blocks any data transfer matching no explicit rule in the DLP policy with the option for user to override the block by requesting an exception

User interface

Administrative user interface

Feature	Feature support/ parameters	Feature description/notes
Aggregate policy view	Yes	Ability to display the DLP policy specified for the entire management domain in a single UI window
Administrative UI types		
Graphical UI	Yes	
Web-based UI	Yes	Cyber Cloud management portal, Cyber Protection service console
Management consoles		
Acronis Cyber Cloud management portal	Yes	Web-based application that enables administrators to monitor the usage of services and access the service consoles, manage tenants and user accounts, configure services and quotas for tenants, manage storage and branding, generate service usage reports
Acronis Cyber Protection service console	Yes	Web-based application that enables administrators to fully manage Advanced DLP and other modules of the Cyber Protection service
Exception	Yes	A default rule with this permission blocks any data transfer matching no explicit rule in the DLP policy with the option for user to override the block by requesting an exception

End user interface

Interactive on-screen notifications	Yes	End users interact with the DLP solution via a set of interactive notification windows popping-up on their workload's screens to inform on DLP actions impacting their business communications and getting their real-time response as necessary
Informational on-screen notifications	Yes	Data transfer denial notification

Log management and analysis

Feature	Feature support/ parameters	Feature description/notes
Configurable DLP audit log retention	Yes	Ability to configure audit log retention period for the company/unit
DLP event viewers		A built-in DLP events viewer allows administrators to view and analyze collected DLP logs for incident investigations, policy tuning and troubleshooting, as well as information security auditing
Audit log viewer	Yes	A viewer of log event records generated by managed DLP agents on end user-initiated operations controlled by DLP policies
Shadow log viewer	No*	A viewer of shadow copies of data carried on in data transfers that matched policy rules with the "Shadow" action set on. * Will be considered for a future update of Advanced DLP in Cyber Protect Cloud if shadow logging is requested by customers. * Considered for support in Advanced DLP as a component of Cyber Protect On-prem
Agent (monitoring) log viewer	No*	A viewer of log of DLP agent service-specific events on managed DLP agents (e.g. agent start/stop, policy changes, local storage issues, etc.) * Will be supported in a future update together with the agent log
Administrative log viewer	No*	A viewer of log containing event records of actions performed by users with administrative roles to manage Advanced DLP * Will be supported in a future update together with the administrative log
Searching in log record parameters	Yes	Ability of log viewer to display only those log records whose parameters contain the text of the search string
Filtering by log record parameters	Yes	Ability of log viewer to display only those log records whose parameters correspond to the criteria of filters supported for these parameters

Reporting

Feature	Feature support/ parameters	Feature description/notes
Report types		DLP usage and event reports
Prebuilt reports with configurable parameters	Yes	Recent DLP events (a widget for monitoring), statistical reports in widgets (4)
Built-in report viewers	Yes	Reports section in Cyber Cloud management portal, Dashboard in Cyber Protection service console, Reports section in Cyber Protection service console
Report export	E-mail	Administrators can send reports as e-mail attachments
Report export formats	Excel, PDF	Administrators can choose report export formats

Management operations security

Feature	Feature support/ parameters	Feature description/notes
DLP audit log retention	Yes	The ability to keep event records in the DLP audit log during the specified retention period without any modification by administrative and non-administrative users
Management communications confidentiality and integrity	Yes	All communications between Acronis Cyber Protect Agents and Acronis Cyber Cloud are confidential and ensure the integrity of transferred management information
Management server authentication	Yes	Acronis Cyber Protect Agents authenticate management servers in Acronis Cyber Cloud when communicating with them
Agent status monitoring	Yes	Operational status of each Cyber Protect Agent is monitored by Acronis Cyber Cloud
Role-based administration		Separation and delegation of administrative roles allow optimizing management operations and reducing the risk of management rights abuse
Super administrator (Company administrator)	Yes	Super administrator can create/manage/delete accounts for users and assign them DLP auditor, DLP agent log administrator, and retention administrator roles.
DLP policy administrator (Cyber Protection service administrator)	Yes	DLP policy administrator can create and manage DLP policy and DLP agent log parameters
Retention administrator (Company or unit administrator)	Yes	Retention administrator can manage audit log retention settings for the company/unit
Auditor (new administrative role)	No*	An administrative role with the following rights: view and analyze DLP audit logs, shadow logs, DLP agent logs, DLP administrative logs, DLP policies, DLP-related related configuration settings, and DLP statistical reports. * Will be supported in a future update.

Product localization

Feature	Feature support/ parameters	Feature description/notes
Administrative user interface	25 languages	
End user interface	25 languages	