Service description

Cyber Protect Cloud
Cyber Protect Appliance

Version	Date	Authors
2.0	29.06.2021	Green Product Management

moving. forward. together.

Contents

1. Service versions

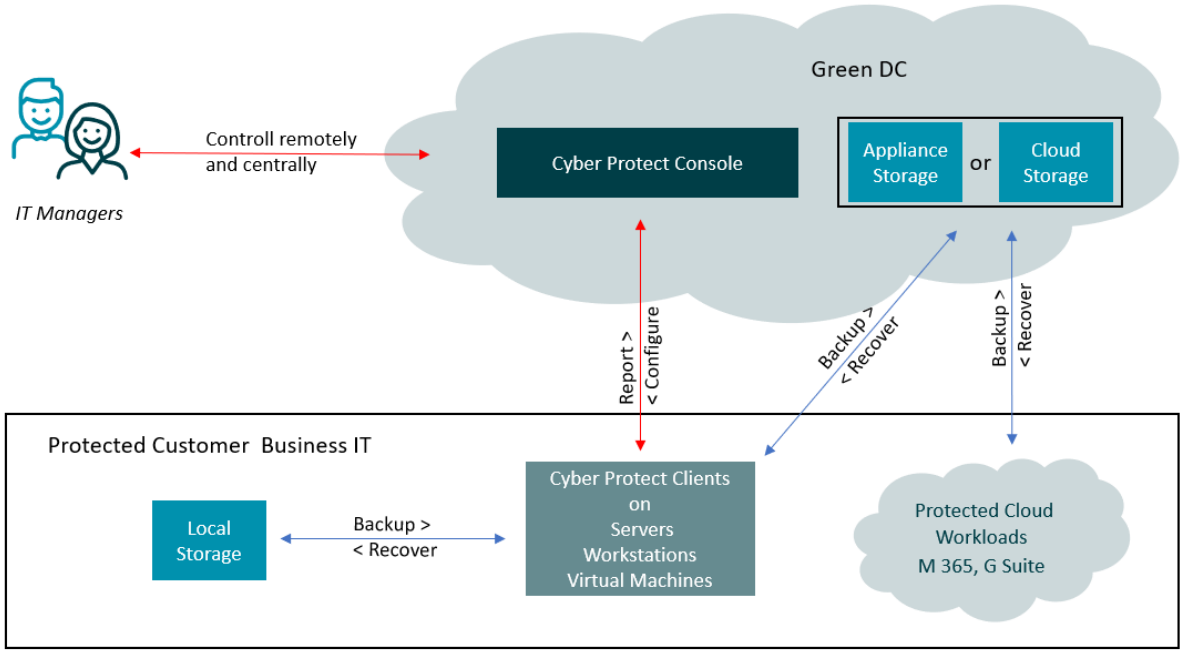
Cyber Protect Cloud combines professional backup functions with next-generation, AI-based anti-malware protection and enterprise-grade endpoint protection management capabilities in a single solution.

The service provides drive-level and file-level backup and recovery to safeguard workloads on more than 20 platforms. The AI-based behavioral engine can detect and stop malware, ransomware and zero-day attacks.

Cyber Protect Appliance allows customers to use the exact same services and features of Cyber Protect Cloud on dedicated hardware. Cyber Protect Appliance comes with various capacity sizes and is perfectly coordinated to the Cyber Protect Cloud solution.

1.1 Service access point

The responsible IT managers are given complete control over the components on offer by means of the Cyber Protect Console.



The Cyber Protect Console is accessible over a regular internet connection.

1.2 Responsibilities

Service provision

- Green is responsible for the Cyber Protect Console and provides the customer with both the cloud storage and the Cyber Protect Clients through its partner Acronis.
- Green provides the necessary information regarding firewall rule sets.
- The customer ensures access to the Cyber Protect Console over the internet.
- The customer ensures that the necessary rule sets are set up on the local network devices (firewalls, routers) to enable the incoming and outgoing data streams.

Service operations (Appliance)

- The customer must ensure that the power supply provided in its own rack is correct (AC input voltage: 230 V, AC input frequency: 50 Hz, max. AC input current: 2 A). Responsibility for downtime caused by a power failure in the customer's rack is explicitly excluded. In the case of an "Appliance-shared or dedicated rack", Green ensures the power supply, the required ambient conditions and access protection.
- The customer must ensure that the ambient conditions on site are correct (operating temperature: 0°C to 40°C, operating humidity: 10% to 85%, non-condensing, ambient air: largely dust-free).
- The customer must protect the Appliance from access by unauthorized third parties. Only authorized operating personnel may have access to the Appliance.

Operating the Cyber Protect Cloud service

- Green will provide the customer with support services for troubleshooting purposes.
- If they notice a fault, the customer must report it to Green using the channels mentioned in section 3. If troubleshooting is required, the customer will actively participate in the error analysis process. The customer is responsible for notifying users about faults.
- The customer must appoint a responsible contact for Green who can make binding decisions on the customer's behalf.
- The customer must report faults in writing in a comprehensible and detailed manner, stating all the information that is useful for identifying and analyzing the cause.
- The customer must provide a log trace or log files of its workloads on Green's request to demonstrate that the workloads are working properly.
- The customer must grant Green's employees access to its premises insofar as doing so is necessary to limit or eliminate faults.
- Green monitors the provisioned Appliance for availability through Business Customer Service (BCS) 365 days a year (24/7).
- Green installs the software updates and patches provided by the Appliance manufacturer in a timely maintenance window (see 2.1).
- Adjustments to the initial configuration, such as changes to firewall rules, are made during business hours following verification by BCS. Configuration changes outside of business hours will be charged separately at the applicable hourly rates.
- Green provides the customer with statistics and log files of the deployed workloads using the Cyber Protect Console. Analysis or interpretation of the log files by Green is subject to a fee.

Termination of the service

- The customer must return all equipment provided by Green for the performance of the service within 30 days of the contract ending, without being prompted to do so, and in proper condition.
- The customer is responsible for all fees and costs associated with this reassignment. The customer may also instruct one of the provider's technicians to collect the equipment for a charge, send it by post or, if necessary, choose another option.
- The customer is liable for damages in the following cases:
  a. If the Appliance is lost or not returned within 30 calendar days after the end of the contract;
  b. If the Appliance is no longer functional due to gross negligence.
  The fee will be at least one year's rent should cases a. or b. occur.

1.3 Service parameters

The service parameters in the table below apply.

1.3.1 Cyber Protect service

Characteristics	Cloud	Appliance
Cloud storage (capacity)	Unlimited	Depending on the model
Availability	99.9%	99.9%
Workloads licensing	Per device	Per device
Storage licensing	Per GB	Included
Basic security (included)	✓	✓
Basic management (included)	✓	✓
Backup	✓	✓
Advanced security	✓	✓
Advanced management	✓	✓

1.3.2 Appliance hardware

Appliance model number	HDD size	Raw capacity	Usable capacity
Model 15031	4 TB	60 TB	31 TB
Model 15062	8 TB	120 TB	62 TB
Model 15078	10 TB	150 TB	78 TB
Model 15093	12 TB	180 TB	93 TB
Model 15108	14 TB	210 TB	108 TB
Model 15124	16 TB	240 TB	124 TB

1.3.3 Appliance locations

The Cyber Protect Appliance can be placed in the following locations in Green's data center. Depending on the location, the customer or Green is responsible for ensuring the required operating environment.

Location	Description	Responsible for the operating environment
Swiss Cube	Operation in the customer's own Swiss Cube rack	Green (shared or dedicated rack)
Colocation	In the customer's own colocation rack or data center cage with an additional switch	Customer

Another fire compartment's shared rack	Rack shared with other customers, incl. power, switch and connection to the customer infrastructure in Green's data center	Green (shared or dedicated rack)
Another fire compartment's dedicated rack	Private rack, incl. power, switch and connection to the customer infrastructure in Green's data center	Green (shared or dedicated rack)
Shared rack (geo-redundant)	Rack in another Green data center, shared with other customers, incl. power, switch and connection (10 Gbit/s) to the customer infrastructure in Green's data center	Green (shared or dedicated rack)
Dedicated rack (geo-redundant)	Private rack in another Green data center, including power, switch and connection to the customer infrastructure in Green's data center	Green (shared or dedicated rack)

1.4 Backup features

1.4.1 Backup and recovery

The Backup module lets you back up and restore physical and virtual machines, files and databases using both local storage and cloud storage as backup destinations.

1.4.2 Compression and deduplication

Compression and deduplication are automatically enabled in the Cyber Protect backup format (*.tibx). This is client-side deduplication ("in-archive") with the aim of eliminating the need to transfer existing data. Depending on how the data is structured, the two methods can save a considerable amount of bandwidth and backup memory.

1.4.3 Replication

You can enable backup replication to have each backup copied to a secondary storage location straight after it is created at the primary backup destination. If previous backups weren't replicated (e.g. because the network connection was lost), the software will also replicate any backups that appeared after the last successful replication. If backup replication is interrupted in the middle of a process, the data that has already been replicated will not be re-replicated the next time replication starts, thus minimizing the time lost.

Replicated backups are independent of backups that remain in the original storage location (and vice versa). You can restore data from any of these backups without having access to other storage locations.

1.4.4 Continuous Data Protection (CDP)

Backups are usually performed with regular but quite long time intervals (for performance reasons). If the system is suddenly damaged, the data that was changed in the period between the last (most recent) backup and the system failure will be lost.

The Continuous Data Protection (CDP) function allows you to back up selected data continuously between scheduled backups.

- By monitoring specified files/folders for changes
- By monitoring the files of specified applications for changes

1.4.5 Forensic data

Malicious programs (e.g. computer viruses, malware or ransomware) can perform malicious activities, such as stealing or altering data. These activities may need to be investigated, but this can only be done if digital evidence is available. However, parts of the digital evidence (e.g. certain files or activity traces) may be deleted – or the machine that the malicious activity took place on may no longer be available.

Backups with forensic data ("forensic backups") allow investigators to examine areas of drives that are not normally included in a traditional drive backup. The Forensic Data backup option allows you to collect the following digital evidence data, which can then be used for forensic investigations: snapshots of unused drive storage space, memory dumps and snapshots of running processes.

Backups with forensic data are automatically digitally authenticated.

1.4.6 Backup scan for malware

The backup scanning functionality allows you to prevent infected files from being restored from backups. Using this functionality allows you to verify that your backups are clean (i.e. not infected with malware). The backup scanning functionality is only supported for Windows operating systems. Backup scanning is performed by the cloud agent in an environment outside of the corresponding end-user machine (i.e. in the Acronis Cloud).

1.5 Security and management features

1.5.1 #CyberFit Score

#CyberFit Score provides a security assessment and scoring mechanism that evaluates a computer's security situation. It identifies security gaps in the IT environment and open attack vectors on endpoints and provides recommendations for improvement in the form of a report. The #CyberFit Score functionality is supported starting with Windows 7 (first version) and Windows Server 2008 R2.

1.5.2 Anti-virus and Anti-malware

The Anti-virus and Anti-malware module can secure your Windows, Linux and macOS devices against all the latest malware threats.

- Detecting malware in files – in real-time mode (Realtime Protection, RTP) as an option or manually executed on demand (On-Demand mode)
- Detecting malicious behavioral patterns in processes (for Windows)
- Blocking access to malicious URLs (for Windows)
- Moving dangerous files to a quarantine folder
- Managing a positive list of trusted enterprise applications

1.5.3 Active Protection

Active Protection monitors the processes running on the protected machine in real time. If a third-party process attempts to encrypt files on the machine or compute a digital cryptocurrency, Active Protection generates an alert and takes appropriate protective measures. Active Protection uses behavior-based heuristics to detect malicious processes. With this approach, Active Protection can also detect new (previously unknown) malware as malware based on typical behavioral patterns.

The Self-Protection function also **prevents** the processes, registry entries, executable files and configuration files of the backup software itself, as well as existing backups stored in local folders, from being modified.

1.5.4 URL filtering

Malware is often spread using malicious or infected websites using the drive-by download method. URL filtering protects devices from threats like malware and phishing by blocking user access to specific websites. The URL filtering database used contains data on websites with disputed information about pandemics, scam URLs and phishing URLs.

1.5.5 Microsoft Defender Antivirus

Microsoft Defender Antivirus is a built-in anti-malware component of Microsoft Windows that has been delivered with the operating system **since** Windows 8.

The Microsoft Defender Antivirus (WDA) module allows you to configure a WDA security policy and monitor its status through the Cyber Protect Console. This module can be used on machines that have Microsoft Defender Antivirus installed.

1.5.6 Quarantine

The quarantine folder is an isolated folder on a client's or a server's internal drive. Suspicious files are stored there. This approach prevents the threat from spreading further. Quarantining allows you to review suspicious and potentially dangerous files on the device and determine how best to proceed.

1.5.7 Vulnerability assessment and patch management

The vulnerability assessment (VA) is a process designed to identify, quantify and prioritize vulnerabilities found in a system under investigation. In the Vulnerability Assessment module, you can have your machines scanned for vulnerabilities to verify whether the operating systems and installed applications are up to date and working properly.

1.5.8 Software and hardware inventory

The inventory function allows you to view all the software and hardware assets available on Windows and macOS devices with Cyber Protect licenses. Creating inventories allows you to:

- Identify the organization's IT assets
- Search the software and hardware inventory of all the devices in the organization
- Compare the software or hardware components on several company devices
- Display detailed information about a software or hardware component

1.5.9 Remote access (RDP and HTML5 clients)

Cyber Protect enables remote access to machines. You can remotely connect to and manage your end-user machines. With the HTML5 client, you can exchange text with the remote machine in both directions using the clipboard (copy and paste). With the RDP client, you can exchange texts and files using the clipboard (copy and paste).

1.5.10 Remote Wipe

Remote Wipe allows the administrator or device owner to delete the data on a managed device. For example, if the device is stolen, any unauthorized access to sensitive information is prevented.

Remote Wipe is only available for computers running on Windows 10.

1.5.11 Monitoring

The dashboard contains a number of customizable widgets that provide a convenient overview of the Cyber Protect solution's ongoing actions. The widgets are updated every five minutes. The current state of the dashboard can be downloaded as a .pdf and/or .xlsx file or sent as an email.

2. Service level agreement

Service availability is defined for each service individually and can be found in the relevant table. All services described in this document are run by the Green BCS and supported by Green's customer service team.

2.1 Operating and support hours

The operating and support hours, plus the fault acceptance times, are defined in the table below.

Service level and target values	Standard support	Business support (24/7)
Operating hours	Monday to Sunday from 12:00 am to 11:59 pm	Monday to Sunday from 12:00 am to 11:59 pm
Maintenance window	Sunday from 2:00 am to 6:00 am Monday from 8:00 pm to 10:00 pm or subject to prior notice	Sunday from 2:00 am to 6:00 am Monday from 8:00 pm to 10:00 pm or subject to prior notice
Support hours	Monday to Friday from 8:00 am to 5:30 pm except on legal holidays	Monday to Sunday from 12:00 am to 11:59 pm
Troubleshooting	Monday to Sunday from 12:00 am to 11:59 pm	Monday to Sunday from 12:00 am to 11:59 pm

Support tickets can be opened through the following channels:

- On the MyGreen portal: my.greendatacenter.ch
- By calling +41 56 460 23 23 during customer support hours
- Using the form on the website: https://www.green.ch/en/contact-form

2.2 Violations of the SLA and credit rules

If Green is unable to provide the defined availability, the customer acknowledges and agrees that the credits agreed to herein shall be the customer's sole and exclusive compensation. A credit is granted as soon as the service availability drops below the guaranteed thresholds and the customer reports this in a support ticket. The outage of one part of a redundant system shall not be considered downtime. Only a correctly opened ticket can be used to calculate downtime and credits.

The table below shows the credits (per year) expressed as a percentage of the basic monthly recurring charges (MRC). These credits and compensations shall be considered final. No other or additional compensation shall be granted. No credit or payment shall be made for any reason or to any extent other than that set out herein, including (but not limited to) loss of business on the Customer's part due to downtime. The credit relates exclusively to the service affected by the fault.

Availability achieved without redundancy	Availability achieved with redundancy	Credit
≥ 99.9%	≥ 99.5%	No credit
≥ 99.8%	≥ 99.95%	10% of the MRC
≥ 99.7%	≥ 99.9%	20% of the MRC
≥ 99.5%	≥ 99.8%	30% of the MRC
Less than 99.5%	Less than 99.8%	40% of the MRC

If the customer wishes to assert any claims against Green, this must be done using the contact form provided at https://www.green.ch/en/contact.

If a service is unavailable for a certain period of time, no SLA credit will be granted if this is attributable, either in part or in whole, to one of the following causes:

1) The malfunction of equipment on the customer's premises (if not owned by Green), at the customer's location (e.g. due to a power failure) or equipment belonging to one of the customer's suppliers
2) Natural disasters, terrorist attacks or other force majeure events
3) An outage due to magnetic/electromagnetic interference or electrical fields
4) Any negligent act or failure to act on the part of the customer (or on the part of the customer's staff, representatives or subcontractors), including:
   a) Delays in the customer's delivery of necessary equipment
   b) Failure to grant Green access to the installations for testing purposes or to perform repairs
   c) Failure to grant access to the customer's facilities to enable Green to fulfill its service obligations
   d) Failure to take appropriate countermeasures regarding the faulty services, as recommended by Green, or the prevention of Green from taking such measures itself
   e) Failure to use redundancies as offered by the service level
   f) Negligence on the part of the customer or willful misconduct, including the customer's failure to follow agreed procedures
5) If the customer prevents or delays access to the cage or data
6) Non-availability due to scheduled maintenance (if the customer has been given prior notice) and emergency maintenance to prevent future downtime
7) Deactivation or discontinuation of the service by Green if the customer has not paid within 90 days of the date of the bill, or for another good cause.

3. Legal provisions

3.1 Establishment of the legal relationship

A legal relationship is established between Green and the customer as soon as the online order placement process has been completed or by way of a quote. Measurement of the SLA parameters begins when the customer successfully logs in to the portal for the first time.

3.2 Compliance with local legislation

The customer must ensure that no illegal data traffic is sent via Green connections. Green assumes no liability for this.

3.3 Restrictions

Compensation for Green's services is limited to the compensation amounts specified in this document. No credit or payment will be made for reasons or of an amount other than those specified here including, but not limited to, any lost business suffered by the customer as a result of downtimes.

3.4 Use of personal data

Customers expressly accept the guidelines issued by Green governing the use of personal data. For more information, please refer to: https://www.green.ch/en/legal-aspects/data-privacy.

3.5 GTC

The General Terms and Conditions of the provider (General Terms and Conditions of Green AG) https://www.green.ch/en/legal-aspects/contract-terms) form an integral part of the customer agreement. The general terms and conditions of the customer shall not apply. Any provisions to the contrary contained in the customer's documents are not applicable. Cancellations, amendments and supplements to the service agreement and the service contracts must be made in writing. Should individual provisions of this service agreement or the service contracts or other appendices to the customer agreement prove to be legally invalid or unenforceable, the invalid or unenforceable provision shall be replaced by a valid or enforceable provision that comes closest to the desired effect of the contracting parties at the time the respective provision was agreed and corresponds to the common objectives set out in the preamble to this service agreement. The new provision may not result in any impairment of the relationship between the provider's services and the customer.

4. Definitions

Term	Definition
Service level	Defined and measurable criteria for Green's provision of a certain quality of service
Service parameters	Desired but not mandatory service metrics
Operating hours	The operating hours are the times during which the system is generally available. Scheduled and announced maintenance windows do not form part of the operating hours. The operating hours are at least 8,712 hours and are calculated as follows: 24/7 for one year = 8,760 h – 48 h maintenance window. If there is redundant architecture, the two redundant devices/facilities are maintained at different times
Support hours	The hours during which the customer can reach a customer service representative or, if the customer receives 24/7 support, a technician on standby.
Availability	Availability [%] = 100 * ((operating hours – scheduled downtime within operating hours) / agreed operating hours). The agreed operating hours do not include time slots for scheduled maintenance windows. Green guarantees the availability on the data center infrastructure. This includes the following levels: the building with supply infrastructure and network. The solutions on the end customer's side must also feature a high-availability design to achieve the high availability on the connection.
Maintenance window	For the purposes of this SLA, scheduled maintenance is required to provide the services or upgrade the infrastructure. Scheduled maintenance windows are defined in advance and announced on status.green.ch if multiple customers are affected. Customers shall also be informed at least 10 working days before the scheduled service interruption caused by the maintenance work. Green shall inform the technical contact that the customer appointed in writing of the scheduled service interruption and the nature of the same by email. This notification shall be valid for all purposes pursued by this document, regardless of the fact that the customer and/or its representatives were unable to receive this notification for any reason, including email system problems or failures, the customer providing incorrect contact details or any other reason.
Emergency maintenance window	Emergency maintenance windows are announced at least 48 hours in advance and posted on status.green.ch if multiple customers are affected.
Service access point	The service access point is the contractually agreed point at which a service is provided to the customer and monitored, and at which the provided service levels are reported.