

Technical Service Level Agreement

CyberHQ.ai

Effective 21st September 2026

This Technical Service Level Agreement ("Technical SLA") forms a Schedule to, and is incorporated into, the Terms of Use between Avertro Pty Ltd ("Avertro") and the Customer, specifically in relation to the CyberHQ.ai services. It sets out Avertro's commitments in relation to the availability and performance of the CyberHQ.ai, and its obligations in the event of security incidents. Capitalised terms used but not defined in this Technical SLA have the meanings given in the Terms of Use or Product Specific Addendum if applicable. In the event of any inconsistency between this Technical SLA and the Terms of Use, the Terms of Use will prevail.

1. Definitions

In this Technical SLA:

Availability: the percentage of time in a given measurement period during which the Avertro CyberHQ.ai production environment (dashboard, API, and backend ingestion pipeline) is accessible to the Customer, excluding Excused Outages. Availability does not measure, and no target is given for, the operational status of individual sensors, extensions, or agents deployed to monitored endpoints — see Section 3.

Core Component: the dashboard, the API, and the backend ingestion pipeline.

CyberHQ.ai: the Avertro CyberHQ.ai platform offered, encompassing all subscription tiers (including Starter, Professional and Ultimate), however described in the Customer's order.

Downtime Minutes: the total minutes in the measurement period during which any Core Component is Unavailable, counted once regardless of how many Core Components are Unavailable concurrently.

Excused Outage: downtime or performance degradation falling within the categories described in Section 5, which is excluded from the Availability calculation.

Maintenance Window Hours: Standard off-peak hours (typically 9:00 PM to 6:00 AM local time in the Customer's primary hosting region), or any time on weekends or local public holidays in that region.

Monitored endpoint: a device, browser, or account on which the Customer has deployed a CyberHQ.ai sensor, extension, or agent.

Scheduled Maintenance: planned updates, optimisations, or routine maintenance performed by Avertro on the CyberHQ.ai cloud infrastructure.

Unavailable: in relation to a Core Component, that it fails to respond successfully to Avertro's monitoring probes for a continuous period of five (5) minutes or more; a period of less than five continuous minutes does not render a Core Component Unavailable.

Updates: bug fixes, patches, and minor improvements to CyberHQ.ai made generally available to Avertro's customer base as part of a standard subscription entitlement.

2. Platform Availability

2.1 Avertro targets a platform Availability of 99.9%, measured over a rolling 12-month for the CyberHQ.ai production environment.

2.2 Availability is calculated as follows:

$$\text{Availability (\%)} = ((\text{Total Minutes in Period} - \text{Downtime Minutes}) \div \text{Total Minutes in Period}) \times 100$$

Excused Outages (as defined in Section 5) are excluded from both the numerator and denominator of this calculation.

2.3 The Availability target applies solely to the Avertro-managed CyberHQ.ai cloud production environment. The following are expressly excluded from this commitment:

- Customer-operated infrastructure, networks, or devices, including monitored endpoints;
- Third-party integrations or APIs connected to the platform by or on behalf of the Customer;
- Preview, beta, sandbox, or evaluation environments;
- Tenants on a trial, free, proof-of-concept, or other unpaid subscription;
- Features designated by Avertro as beta, preview, or early access, regardless of the environment in which they are made available; and
- Periods of downtime attributable to Excused Outages.

3. Monitored Endpoint Coverage (No Service Level)

3.1 CyberHQ.ai's sensors, extensions, and agents run on Customer-managed endpoints, browsers, and networks that Avertro does not control. Accordingly, Avertro does not commit to a specific uptime or reporting-rate percentage for monitored endpoints, and this Section is not a Service Level target in the same sense as Section 2.

3.2 Avertro will:

- monitor the health of the backend ingestion pipeline that receives data from sensors/extensions as part of the Availability commitment in Section 2;
- use commercially reasonable efforts to investigate any reported, material loss of monitoring coverage that is attributable to the services rather than the Customer's environment; and
- treat a confirmed, service-attributable monitoring coverage loss as a Severity 1 incident under the Support Policy, regardless of whether it also constitutes a platform outage under Section 2.

3.3 **Continuity of capture.** Where a Core Component is Unavailable, sensors, extensions, and agents continue to capture events on the monitored endpoint, buffering them locally for delivery once the platform is available again. Buffer size and (depending on sensor type) maximum event age vary by sensor type and are available to the Customer on request; once a limit is reached, the oldest buffered events are discarded first. Avertro does not warrant delivery of events lost because the monitored endpoint itself was offline, powered down, or its sensor, extension, or agent was removed, disabled, or blocked.

3.4 **Continuity of enforcement.** Where enabled, DLP policy enforcement continues on the monitored endpoint while a Core Component is Unavailable, applying the most recent cached policy; any policy change made during that period takes effect only once that endpoint next resynchronises with the platform.

4. Scheduled Maintenance

4.1 Avertro reserves the right to perform Scheduled Maintenance on the CyberHQ.ai platform from time to time, prioritising the Maintenance Window Hours applicable to the Customer's designated hosting region.

4.2 Avertro will provide at least 48 hours' advance notice for routine Scheduled Maintenance expected to affect Availability. For Major Maintenance (defined as architectural updates, API breaking changes, or maintenance

anticipated to cause extended downtime exceeding 2 hours), Avertro will provide at least 7 to 14 calendar days' advance notice via the Customer Support Portal and/or email to the Customer's registered technical contact. Avertro will use reasonable endeavours to minimise the duration and frequency of Scheduled Maintenance.

4.3 Avertro may perform emergency maintenance outside the Maintenance Window, and without advance notice, where reasonably necessary to preserve the security, integrity, or stability of the platform. Avertro will notify affected Customers as soon as reasonably practicable and use commercially reasonable efforts to minimise disruption.

4.4 Downtime attributable to Scheduled Maintenance does not count toward the Availability calculation and does not constitute a breach of this Technical SLA.

5. Excused Outages

Downtime or performance degradation falling within the following categories is excluded from the Availability calculation and does not give rise to any service credit or breach:

Category	Description
Scheduled Maintenance	As described in Section 4.
Force Majeure	Events outside Avertro's reasonable control, including natural disasters, acts of government, or widespread network outages.
Third-party infrastructure	Outages or degradation caused by third-party infrastructure, platform, or service providers (including cloud infrastructure providers such as AWS and GCP, and third-party AI model or API providers) not attributable to Avertro's configuration or architecture.
Customer-caused	Downtime caused by acts, omissions, misconfiguration, or infrastructure failures attributable to the Customer or its users.
Monitored-endpoint environment	Sensor, extension, or agent malfunction caused by the monitored endpoint's own browser, operating system, network configuration, or an end user disabling, blocking, or circumventing the sensor/extension — where not attributable to a defect in the services.
Third-party platform changes	Suspension, removal, or policy change by a browser vendor, extension store, or operating system vendor that impairs the distribution or operation of a sensor, extension, or agent.

Avertro will use commercially reasonable efforts to minimise the impact and duration of any outage, including those caused by third-party infrastructure providers, and will communicate status updates to affected Customers through the Customer Support Portal where practicable.

6. Performance Standards Summary

Metric	Target	Measurement Period	Notes
Platform Uptime	99.9%	Rolling 12 months	Excludes Excused Outages
Scheduled Maintenance window	Within Maintenance Window Hours wherever practicable	As required	Advance notice per Section 4

7. Platform Monitoring and Status Communication

7.1 Avertro maintains continuous internal monitoring of the CyberHQ.ai cloud production environment. Where Avertro detects a material degradation in platform performance or Availability, it will endeavour to:

- publish a status update via the Customer Support Portal; and
- notify affected Customers via email to their registered technical contact, where the outage is expected to exceed 30 minutes.

7.2 Avertro does not guarantee real-time public status page availability as part of this Technical SLA, but will use reasonable efforts to communicate incident status and estimated resolution timelines.

8. Security Incident Notification

8.1 In the event that Avertro's security operations team detects a confirmed security incident actively involving CyberHQ.ai Customer data, Avertro will communicate with the affected Customer regarding the incident's operational impact under Section 7.

8.2 Where a security incident involves a Personal Data Breach affecting data collected from Monitored endpoints or other personal data, the notification timeframe and required content are governed exclusively by the applicable Data Processing Addendum for CyberHQ.ai — this Technical SLA does not separately state, restate, or vary that timeframe.

9. Policy Review

This Technical SLA is subject to periodic review. Avertro may update this from time to time. We will inform you if we make a material change via email or an in-platform notification. The current version of this Technical SLA is available on the website.

This Policy was last reviewed in September 2026 and supersedes all prior versions of Avertro's Technical SLA insofar as they applied to CyberHQ.ai.