



Avaris One – Whitepaper

Secure mobile monitoring for Avantra environments.

Private project. No warranty. No legal advice.

Inhalt / Contents

1. English Version
2. Deutsche Version

1. English Version

Overview

Avaris One is a private iOS app that connects to an Avantra backend and shows monitoring information. The app is designed as a viewer only. It does not store operational system data on the device. All monitoring data is fetched live from the Avantra GraphQL API.

High level architecture

The architecture is simple and secure: Avaris One app -> HTTPS or HTTP -> Avantra GraphQL API -> Avantra backend. No extra servers, relays or analytics services are involved.

Security model

- HTTPS/TLS is used by default.
- HTTP can be enabled manually for test systems.
- The API token is stored only in the iOS Keychain.
- No data is ever sent to third party servers.
- The Avantra role model is fully respected.

Local data storage

Avaris One follows a strict minimal-storage principle. Only technical configuration required for connectivity and UI behavior is saved on the device.

What is stored locally

- API Token, stored exclusively in the Apple Keychain.
- Server configuration: URL, namespace, display name, HTTPS/HTTP setting.
- User interface preferences such as selected server or theme.

What is NOT stored locally

- System lists.
- Check results, histories or health states.
- Workflow data.
- Database lists.
- Metrics, logs or performance values.
- Any personal data from Avantra.
- Analytics, telemetry or crash data.

Behavior when access is removed

If access to the Avantra server is removed, the app simply shows no data on the next reload. Because Avaris One stores no operational data, nothing outdated can be displayed.

Transport security

HTTPS/TLS is enabled by default. Users may enable HTTP manually for non-TLS test systems. This setting is saved per server and reduces transport security.

No third-party processing

Avaris One communicates only with the configured Avantra server. There is no analytics, no tracking and no external data processing.

Features overview

- On-device security with Keychain-based storage.
- Clean navigation for systems, servers, databases and workflows.
- Workflow control with role-based restrictions.
- Built-in support without analytics.
- Dark-first minimalistic design.
- No ads, no tracking, no third-party SDKs.

Use cases

- On-call engineers checking system health.
- Quick views on checks and workflows.
- Read-only access without local system data.

Compliance and privacy

Avaris One does not introduce additional personal data. It follows principles of data minimisation and purpose limitation. No analytics or tracking is used.

Privacy policy link

<https://avarisone.de/privacy.html>

Disclaimer

This is a private software project. No warranty is given for correctness, security or legal compliance.

2. Deutsche Version

Übersicht

Avaris One ist eine private iOS App, die sich mit einer Avantra Umgebung verbindet und Monitoring Daten anzeigt. Die App speichert keine operativen Systemdaten, sondern lädt alle Informationen live über die GraphQL API.

Architektur

Avaris One App -> HTTPS oder HTTP -> Avantra GraphQL API -> Avantra Backend. Es werden keine zusätzlichen Server oder Analyse Dienste genutzt.

Sicherheitsmodell

- Standardmäßig wird HTTPS/TLS verwendet.
- HTTP kann manuell für Testsysteme aktiviert werden.
- Der API Token wird ausschließlich in der iOS Keychain gespeichert.
- Es gibt keine Datenübertragung an Drittserver.
- Berechtigungen aus Avantra werden vollständig respektiert.

Lokale Datenspeicherung

Avaris One folgt einem konsequenten Minimal-Speicher-Prinzip. Es werden nur technische Einstellungen gespeichert, die für die Verbindung und Bedienung notwendig sind.

Was lokal gespeichert wird

- API Token (in der Apple Keychain).
- Serverkonfiguration (URL, Namespace, Anzeigenname, HTTPS/HTTP Einstellung).
- UI Einstellungen wie ausgewählter Server oder Theme.

Was NICHT lokal gespeichert wird

- Systemlisten.
- Check Ergebnisse, Status oder Historien.
- Workflow Daten.
- Datenbanklisten.
- Metriken, Logs oder Performance Daten.
- Personenbezogene Daten aus Avantra.
- Analyse-, Tracking- oder Telemetriedaten.

Verhalten bei Entzug des Zugriffs

Wenn der Zugriff eines Benutzers entfernt wird, zeigt die App beim nächsten Reload keine Daten mehr an. Avaris One speichert keine operativen Daten, daher können keine veralteten Informationen angezeigt werden.

Transportsicherheit

Standardmäßig nutzt die App HTTPS/TLS. HTTP kann manuell aktiviert werden, reduziert jedoch die Sicherheit.

Keine Weitergabe an Dritte

Es findet keinerlei Übermittlung an Drittanbieter, Analyseplattformen oder Trackingdienste statt.

Funktionen

- Sicherheit auf dem Gerät durch Speicherung in der Keychain.
- Klare Navigation für Systeme, Server, Datenbanken und Workflows.
- Workflow Kontrolle mit Rollenkonzept.
- Integrierter Support ohne Analytics.
- Dark First Design.
- Keine Werbung, kein Tracking.

Compliance und Datenschutz

Die App folgt den Grundsätzen der Datenminimierung und Zweckbindung. Personenbezogene Daten werden nicht zusätzlich verarbeitet.

Link zur Datenschutzerklärung

<https://avarisone.de/privacy.html>

Haftungsausschluss

Dies ist ein privates Softwareprojekt. Es wird keine Haftung übernommen.