Ordantra

PRODUCT DATASHEET · ENDPOINT OPERATIONS

Ordantra Agent and Companion

Continuous endpoint intelligence and consent-led support for service teams, paired with a safe, useful Windows experience for the people using those devices.

SIGNED-IN USER

Ordantra Companion

Status · prompts · support consent

Protected local IPC

TRUSTED WINDOWS SERVICE

Ordantra Agent

Inventory · posture · signed heartbeats

Outbound HTTPS 443

WORKSPACE ISOLATED

Ordantra Cloud

Assets · risk · service workflows

15 min
Standard heartbeat interval

Per device
Independent protected identity

HTTPS
Outbound-only cloud communication

10 min
Attended-support request expiry

TWO COMPONENTS. ONE TRUSTED BOUNDARY.

Deep visibility without handing desktop users privileged access.

The Agent performs trusted machine-level work. The Companion supplies the human touchpoint. They communicate locally; only the Agent holds the endpoint identity used with Ordantra.

01

Ordantra Agent

A resilient background service that turns endpoint state into current, structured asset and risk intelligence.

Asset intelligence

Hardware, operating system, installed software, users and device identity.

Security posture

Encryption, firewall, secure boot, TPM and security-product signals.

Reliable check-in

Signed, sequenced heartbeats report endpoint health and inventory every 15 minutes.

Risk automation

Policy matches can surface endpoint risk and create actionable service work.

Managed updates

Platform-specific releases, verified payloads, outcome reporting and rollback safeguards.

Attended support

Consent responses and support state cross the same authenticated Agent boundary.

02

Ordantra Companion

A windowless, per-user Windows tray application designed for clarity and controlled interaction.

Visible status

A lightweight Windows tray experience shows connection and Agent version.

User actions

Check now and approved update actions without exposing privileged credentials.

Secure prompts

Ownership and compliance interactions cross an authenticated local service boundary.

Optional usage insight

Foreground-application summaries are collected only when a workspace enables the feature.

User-approved support

Shows the technician and reason, with accept, decline and end-session controls.

ATTENDED REMOTE SUPPORT

Desktop assistance starts with a person saying yes.

An authorised administrator requests support from the asset record. The signed-in user sees who is asking and why before any desktop content or control becomes available.

Explicit, expiring consent

Requests expire after ten minutes. The user can accept or decline; there is no timeout, locked-device or no-user auto-accept path.

Visible and revocable

A persistent privacy bar identifies the active session. The endpoint user can end access at any time.

Bounded transport

The trusted service verifies the approved transport against its pinned SHA-256 digest. Technicians receive an expiring guest session rather than a standing transport account.

SECURITY BY DESIGN

Built to protect fleet identity and minimise credential exposure.

Enrolment exchanges a workspace key for a unique device credential. The raw enrolment credential is not retained, and the Windows Agent protects its derived signing key with machine-scoped DPAPI.

Authenticated heartbeats

HMAC signatures and monotonic sequences protect device messages.

Least-exposed Companion

No Ordantra cloud credential is stored in the tray process.

ACL-protected IPC

Local communication is bounded to the trusted Agent service.

Controlled updates

Signed commands, SHA-256 verification and platform isolation.

Audited support

Requests, consent responses and session opening are recorded against the endpoint and asset.

Tenant isolation

Endpoint data remains scoped to its enrolled workspace.

PRIVACY AND CONTROL

Useful telemetry, with deliberate boundaries.

Collected by default

Device identity, operating system, hardware, installed software, service health and selected security-posture signals.

Workspace controlled

Application-usage summaries are disabled unless explicitly enabled during enrolment or by approved policy.

Not continuous surveillance

No keylogging or microphone capture. Desktop viewing or control is limited to an explicit, visible attended-support session approved by the endpoint user.

DEPLOYMENT PROFILE

Designed for straightforward fleet rollout.

Windows x64

COMPONENTS
Native Agent service + per-user Companion

DEPLOYMENT
MSI, interactive or silent

CONNECTIVITY
Outbound HTTPS 443

Linux

COMPONENTS
Agent

DEPLOYMENT
Platform installer + systemd

CONNECTIVITY
Outbound HTTPS 443

macOS

COMPONENTS
Agent

DEPLOYMENT
Platform installer + launchd

CONNECTIVITY
Outbound HTTPS 443

Administrator rights are required for installation and enrolment. The Windows package supports in-place upgrades and service recovery. General-distribution Windows releases are gated on a valid, timestamped Authenticode signature; unsigned packages remain controlled internal previews. Exact supported operating-system versions and current packages are provided in Ordantra Agent settings.