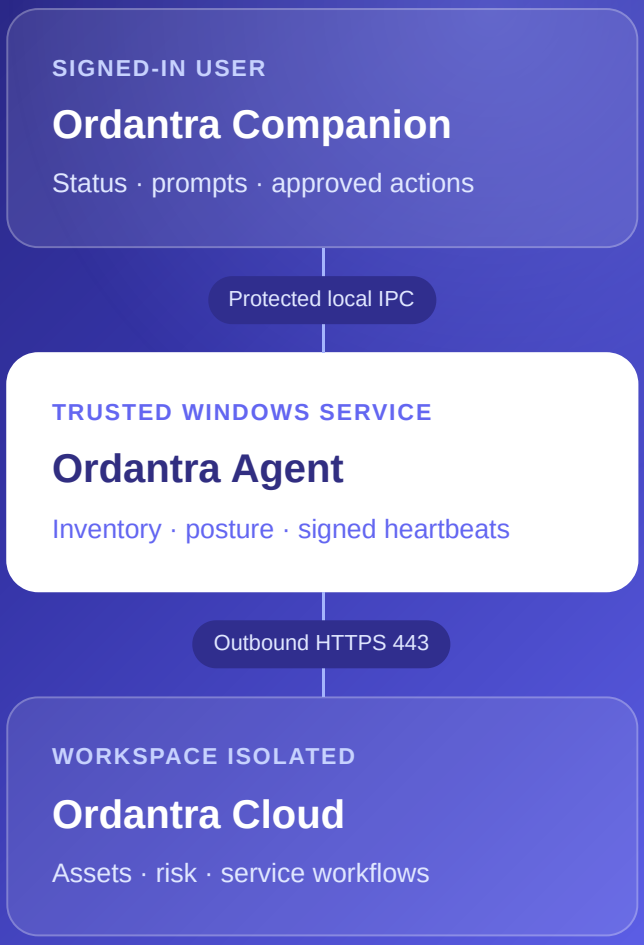
Ordantra

PRODUCT DATASHEET · ENDPOINT OPERATIONS

# Ordantra Agent and Companion

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




**15 min**
Standard heartbeat interval

**Per device**
Independent protected identity

**HTTPS**
Outbound-only cloud communication

**Policy led**
Optional collection and automation

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.

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.

SECURITY BY DESIGN

# Built to protect fleet identity and reduce endpoint trust.

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.

### 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 a surveillance tool

The Agent does not provide arbitrary screen capture, keystroke recording, microphone access or unrestricted remote control.

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. Exact supported operating-system versions and current packages are provided in Ordantra Agent settings.