

Remote Management & Security Model

HOW WE MANAGE YOUR SEALED UNIT

A sealed box. Total privacy. Fully managed.
Yes — it's possible.

Dominion is designed on a simple rule: the box never accepts an inbound connection. Every interaction is initiated by the box, outward — or by you, on site. We can't "log in" to your unit from our office even if we wanted to.



One-way glass: the box calls us, we never call the box.
Your firewall can verify that nothing can reach Dominion from the outside.

How it works — Four outbound-only mechanisms

1



Status checks (outbound telemetry)

On a schedule, Dominion sends a small heartbeat to our management endpoint: service up/down, temperatures, disk space, last night's jobs.

- ✓ Outbound only: your firewall allows egress to one address — our console — and denies everything else.
- ✓ Content-free: only operational signals are sent. No documents, prompts or data ever leave your site.

Even if our office were compromised, there's nothing to steal and no path into your files.

2



Routine fixes & patches (pull-based)

When something needs doing (restart a service, apply a security patch), we place a signed instruction on our server.

- ✓ On its next check-in, Dominion pulls the instruction.
- ✓ It verifies the signature, executes it, and reports the result.

Same direction rule: the box reaches out and asks "anything for me?" Nothing reaches in.

3



Model & software updates (verified)

New models or software are staged on our side. Dominion pulls them, verifies the checksum/signature, validates against your test set, hot-swaps and keeps the previous version for instant rollback.

- ✓ Updates flow to the box.
- ✓ Client data never flows back.

For true air-gapped clients (zero network egress), updates arrive via encrypted USB on a scheduled visit — a tier we offer.

4



Live support (client-initiated)

If a problem needs hands-on work, someone at your firm starts the session (one click).

- ✓ A temporary outbound tunnel opens.
- ✓ We work.
- ✓ It closes.
- ✓ You authorise and can watch every session.

There is no persistent remote access between sessions.

The direction rule in action

YOUR ENVIRONMENT

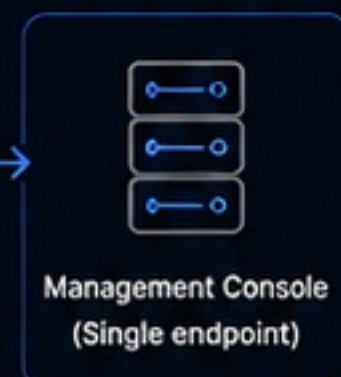


No inbound connections accepted. Ever.

Outbound only
Heartbeat, updates, commands, support (session start).

ENCRYPTED CHANNEL (TLS 1.3)

ERMOS MANAGEMENT



We never initiate connections to the box.

Why this model is secure



Data can't get out.

The channel carries only operational telemetry and commands — never your business data.



Maintenance can still get in.

The box does all the reaching.



Worst-case outcome is safe.

If the box loses its network connection, nothing is exposed. It simply runs stale until reconnected.



No inbound listeners. No open doors.

Unlike conventional remote tools (RMM with inbound admin rights), there is no attack path into your network.



In one sentence

Outbound-only allow-listed egress, content-free telemetry, pull-based command queue, signed updates with rollback, client-initiated ephemeral support sessions, no inbound listeners.

PRIVATE AI INFRASTRUCTURE.
COMPLETE CONTROL.
ermos.com.au