GUARDIAN PLUS

Three network postures for the networks that don’t allow much

How to place a management plane on a segmented or regulated network, and what each choice costs you.

Most platforms give you one topology and expect your network to accommodate it. This guide documents three, from the simplest to one where the management plane sits behind a single inbound rule you can close entirely. It is written for the person who has to answer the firewall change request, not the person who signs the order.

First, what the agent does and does not need

Every managed endpoint dials out over TLS and keeps one authenticated socket open. Nothing listens on the endpoint. Browser terminal, remote desktop, monitoring data and commands all ride that one outbound connection. There is no firewall rule to add on the endpoint, no port to forward, no VPN to maintain.

The endpoint needs outbound HTTPS on port 443 to the management server and must be able to validate its certificate. Intercepting proxies that re-sign TLS are the most common cause of a client that will not connect.

- Windows (desktop and server, 64-bit), macOS (Intel and Apple Silicon), Linux (Ubuntu 22/24, Rocky 9/10, CentOS Stream 9, SUSE 16)
- Signed installers that bundle their own runtime
- Exponential backoff, sleep and wake detection, fast reconnect from suspend

Posture 1: one trusted network

Everything on one trusted network. The management plane and the endpoints already share a security boundary, so the only rule is the outbound one the endpoints already have.

- Fastest to stand up
- No inbound rules on endpoints
- Suited to a single office or data centre

Choose it when your management plane and your endpoints are already inside the same boundary and you are not answering a questionnaire about it.

Posture 2: roaming workforce

Endpoints anywhere: home, hotel, client site. The management console itself stays restricted to your office network or VPN. Agents reach in from any network; console access stays behind your perimeter.

- Agents reach in from any network
- Console access stays behind your perimeter
- No endpoint ever exposed to the internet

Choose it when technicians and machines travel but the people who administer the platform do not need to.

Posture 3: isolated management network

The monitoring plane sits on a private network with exactly one inbound rule. Close even that, and you trade nothing but a delay of up to an hour before a revoked session stops working.

- One inbound pinhole, and it is optional
- Documented tail: sessions expire within the hour
- Built for segmented and regulated environments

Choose it when a regulator, a client contract or your own policy says the management plane cannot be reachable from the networks it manages.

Where a port does open

Each of these is optional and scoped to a machine you choose. None of them is on a managed endpoint by default.

- A collector (an agent promoted to reach devices that cannot run one: switches, firewalls, printers, appliances) binds a local port to proxy for them
- A machine you designate as a trap receiver listens for SNMP traps from your network devices
- Remote desktop on macOS and Linux uses the operating system’s own screen-sharing service on loopback, relayed out over the agent’s existing connection

Single-tenant, always

There is no shared cloud instance. Every customer gets their own deployment: on your hardware, in your cloud account, or hosted by us on infrastructure dedicated to you. Your database, your keys, your instance.

Self-hosting is a deployment choice, not a licensing one. Install with the OS installers (Rocky, Ubuntu or SUSE) or run the container images. Nothing phones home except a daily licence check.

The bad day: what we publish

Our deployment documentation includes a written threat model for total compromise of the management plane: what an attacker would reach, what stays out of reach, and what each posture costs you if it happens. Ask for it during evaluation. Most vendors will send you a certification badge instead.

Bring your firewall team

A technical deep-dive is sixty minutes on your own network diagram: which posture fits, what the change request says, and what the threat model means for you. Book it at https://get.guardianplus.ai/demo.