

One agent on the device, one console above it.

What the agent runs on, where the console lives, and how data moves between them. Start here before your security review.

Windows and macOS, with the same feature set

The same agent capabilities, the same library and the same console on both, so a mixed fleet is one estate, not two.

PLATFORM	WHAT THE AGENT DOES THERE
Windows and macOS	Measure: telemetry, anomalies and the experience score. Fix: on its own, offered to the employee, run by the desk, or scheduled. Govern: software, patches and policy, with the audit log.
Linux	Most of the macOS feature set. Details vary by distribution.
Android	Kiosk mode, device management, data collection and the experience score.
iOS	Data collection and the experience score. Narrower than Android, because Apple limits what an agent can do on iOS.
VDI	Device monitoring, automation and the experience score.
ChromeOS	In proof of concept.

On Windows, that means Windows 10, Windows 11 and Windows Server. Supported versions differ by platform and distribution: [ask us for the versions you run](#).

SaaS by default, or on your own infrastructure

The agent is the same everywhere. What changes is where the server and its data run.

SaaS	On-premises	Air-gapped
Runs on AWS by default, with Azure and GCP customer environments also supported, in the region set for your deployment.	Runs in your own data centre, with the deployment architecture tailored to your infrastructure.	Possible, with a design that covers disconnected operation, licensing, updates, dependencies and telemetry.

Many tenants, one platform. The platform is multi-tenant, with per-tenant branding and licence pools, so a service provider runs every client from one console. The agent side never changes; only the server's place does.

How data moves, and who can see it

The agent reports to your tenant on the Nanoheal server, and one console above it serves every site. These controls ship in the product.

CONTROL	IN THE PRODUCT
Agent to server	Secured with mutual TLS.
Tenancy	Each customer or business unit is a site, with data scoped to each site, with requests for another site refused.
Access	Role-based access, MFA and a full audit log, with SAML and OIDC single sign-on.
Secrets and keys	Secret fields stripped from responses and redacted from logs; site-scoped API keys, stored only as hashes.
AI	Haya, Nanoheal's AI and analytics, runs on your choice of model, including a locally hosted one, behind approval gates, role-based access, execution traces and PII masking.
Residency and retention	Hosted in the region set for your deployment, with retention and deletion agreed with each customer, by deployment and contract.

What sits on the device

What it can do

It works from a fixed set of signed actions. A new fix is a set of parameters for those actions, and each flow passes a check that stops anything incomplete before it is staged.

Footprint

The agent footprint stays flat as automations are added, because each fix uses capabilities the agent already has.

What it measures

Endpoint and digital-experience telemetry, for monitoring, analytics, troubleshooting and automated fixes. Scores are built from a default set of metrics across device, application and network health.

Offline

Fixes and policies keep running without a cloud connection, where the policy or automation does not need one.

For your review. Measured figures, installation and update methods, and signing detail are in our technical whitepaper, shared on request: nanoheal.com/demo/whitepaper. We provide field-level collector detail, shared through our technical and security review process; write to security@nanoheal.com.