

Security by design

How OPS4 protects your systems, your data and your evidence

OPS4 watches and maintains the systems your business runs on: SAP, databases, servers, hypervisors and network devices. A tool with that reach must be at least as well protected as the systems it looks after. This folder explains, without technical jargon, the measures that are built into OPS4 for every customer: not as an add-on, but as part of how the product works.

✓ Isolated

your own instance, your own keys

✓ Controlled

MFA, roles and approval

✓ Recorded

a tamper-evident trail of every action

✓ Verified

signed updates, tested releases

1 Your own environment

- Every customer gets a separate OPS4 instance: its own application, database and encryption keys. Nothing is shared with other customers.
- An instance is delivered empty. Your data, users and configuration are yours alone.
- Secrets entered in OPS4 (passwords, private keys, PINs) are stored encrypted and are never shown again after they have been saved.

2 Who gets in

- Multi-factor authentication with an authenticator app, which an administrator can make mandatory per user.
- Optional allowlist of locations: a sign-in from an unknown address must be confirmed first. The check runs on every request, so a stolen session cookie does not work elsewhere.
- Permissions per user group, per area: view or manage. Running an automation is a separate right from managing it.
- The last administrator account can never be removed or demoted by accident.

3 Everything is recorded

- An audit trail of every change and every action: who, what, when and from where. It cannot be edited or deleted from the application, and is retained for two years.
- Entries are sealed in a hash chain and counter-signed outside the instance, so later tampering is detectable. Your auditor can verify the chain independently.
- A separate access log of every sign-in attempt, including failed ones, shown right in the menu.
- Sensitive values are masked in the trail; it can be read and exported, never altered.

4 Agents you can trust

- Agents on your servers only connect outwards over encrypted HTTPS. No ports need to be opened towards your servers.
- Agent updates are digitally signed. Before installing, an agent verifies the signature against the OPS4 release registry, and refuses the update if it does not match.
- Every instruction an agent receives is checked against a strict list of what is allowed before anything runs.

5 Automation under your control

- Automation is off by default. It has to be allowed twice: when the agent is installed, and per server in OPS4.
- Every automation job goes through an approval step and is logged step by step, with the result kept on record.
- Servers are put in maintenance automatically while a job runs, so alerts and service reports stay correct.
- Major changes, such as an operating system release upgrade, are first tested on an isolated copy without network access, with a snapshot to go back to.

6 Log retention (optional)

- The logs of your servers are kept in a write-once archive: once stored, nobody can change or delete them before the retention period ends, not even an administrator.
- Numbered lines expose gaps, and tripwires alert immediately when, for example, an audit log is cleared or a new administrator appears.
- Logs are encrypted per source and per month, so a specific part can be destroyed when the law requires it. Destroying logs always takes two people.

7 Connections to your other tools

- Integrations read through a separate read-only token, which can never change anything.
- A read token only works from addresses you have allowed. An empty list refuses everyone.

8 How we build OPS4

- Every release passes the complete automated test suite before it can be built, and is delivered as a numbered, verified release.
- OPS4 checks its own components for known vulnerabilities, just as it does for your servers.
- Security reviews are part of our development cycle; findings are fixed in the product, not worked around.
- AI features are optional and are only switched on for an instance on request.

Evidence for your audits

OPS4 helps you produce the evidence that frameworks such as ISO 27001 ask for: who had access, what changed, when systems were down and why, whether backups ran, and which logs were kept. Service level reports include a compliance chapter that brings this together.

Questions about security, or a detailed review with your security officer? We are happy to go through it with you.