PrintFleet

SECURITY WHITEPAPER · OCTOBER 2026

Nothing to open. Nothing to share.

How PrintFleet watches a dealer's copiers and printers without opening a client's network, and keeps every dealer's and client's data apart. For the IT people who review it.

0	0	443	0
open ports at the client	firewall changes or VPNs	outbound HTTPS, and nothing else	documents or print jobs ever read



443 TCP	161 UDP	Printer's web port	17745 TCP	Inbound
out to the hub, the only way off the network	SNMP to the site's printers, and the ranges set to look for new ones	usually 80 or 443, only while a Remote Device Link is open	the status page, on 127.0.0.1 only	none

01

On the client's network

- The agent calls the hub over HTTPS on port 443. Nothing calls in, so no port, firewall rule or VPN is needed.
- It reads printers over SNMP, read only: counters, supply levels, status, serial number and model.
- It never sees documents, print jobs, file names or who printed what.
- Its one local status page answers only on that PC (127.0.0.1) and never shows a credential.

02

The agent's credential

- Each site's agent has its own token. The hub keeps only a SHA-256 hash of it, so it cannot be read back out.
- Install links expire, and making a new one replaces the old.
- Updates come from the hub alone, over HTTPS, and a dealer can switch automatic updates off.

03

Remote Device Link

- Shows a technician a printer's own web pages, over the agent's same outbound connection.
- Only this site's own printers: the hub asks for nothing else, and the agent refuses any other address.
- Open only to people allowed to edit that printer.
- Every link opened is recorded in the audit log.

04

Dealers and clients kept apart

- Every dealer is a separate tenant, and every page and answer is filtered to it.
- A client's people see only their own account and its branches.
- The fleet assistant keeps the same limits, even when a question tries to talk it out of them.
- More than 1150 automated tests, run before every release, include these boundaries.

05

Signing in

- Passwords are stored only as scrypt hashes.
- Optional two-step sign-in with an authenticator app, with one-use recovery codes.
- Five wrong passwords lock that address for 15 minutes.
- HTTPS-only cookies, a CSRF token on every form, and an audit log of sign-ins and changes.

06

Where the data lives

- Hetzner, Nuremberg, Germany, on Auto AI's own server. PrintFleet runs as its own unprivileged service with its own database, in a locked-down sandbox.
- HTTPS everywhere, and server access by SSH key only.
- A backup before every release, and encrypted offsite copies every night, kept for 14 days.

POPIA

Printer data is not personal information. Personal information is about people: those who sign in or are notified, account and site contacts, the audit log and typed notes. The dealer is the responsible party and PrintFleet the operator, under an operator agreement each dealer can sign. Hosting in Germany is a transfer under section 72, to a GDPR country.

Kept no longer than needed

Every reading	90 days, then each printer's first and last of each day
Agent activity log	28 days
Assistant conversations	7 days

Live status, checked every minute: **status.printfleet.co.za**

Checked against the live system on 18 October 2026. **printfleet.co.za**