Security & IT whitepaper

Last updated November 15, 2026

Summary

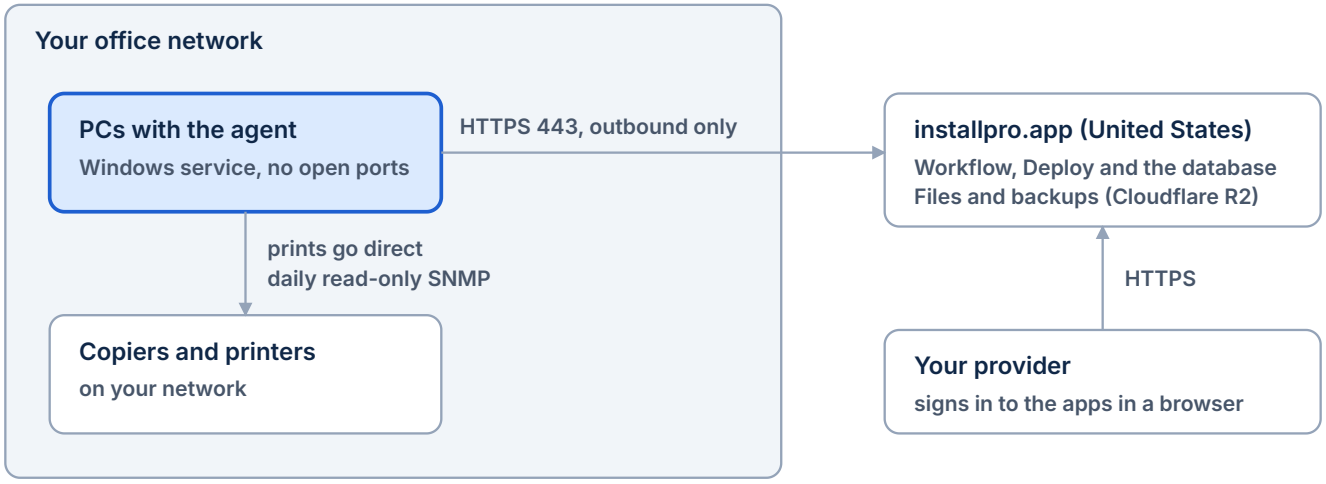
installpro.app is a set of apps used by the company that looks after your printers and copiers (your **provider**, such as a copier dealer or IT company): **Workflow** to plan your installation with you, **Deploy** to set up and look after the printers on your office's PCs without visiting each desk, and **Convert** to move your copier's address book to the new machine. Only Deploy puts anything on your PCs. For IT, the short answer is:

- **The agent only connects out.** A small Windows service on each PC calls installpro.app over HTTPS (port 443) about once a minute, and keeps one request open so new printer jobs reach it right away. It opens no port to the network and accepts no incoming connections.
- **Each PC has its own key.** A PC joins with your organization's activation code once, then uses its own key, readable only by Windows and administrators.
- **It does one job.** It installs and removes printers your provider has set up for you, and once a day reads copiers' model, toner and page counts. It does not read documents, files, browsing or keystrokes.
- **Workflow and Convert install nothing.** They run in a web browser. Convert works on address books inside the browser; only the ones a provider chooses to save are stored, and never with their passwords.
- **Your provider sees only their own customers.** Each provider's information is kept separate from every other provider's.
- **Hosted in the United States**, with HTTPS everywhere, nightly backups and no advertising or tracking.

The rest of this paper explains each point in detail, with a firewall and deployment checklist in section 7.

2. How it works

PCs only connect out, and printing stays on your network



Your provider sets up your printers and drivers in installpro.app Deploy. Each PC's agent checks in over HTTPS, picks up printer installs, and installs them; print jobs then go straight from the PC to the copier and never pass through installpro.app.

3. The Windows agent

The agent is one program, installed to `C:\Program Files\installpro.app` and run as a Windows service called **installpro.app agent**. It starts with Windows and runs whether or not anyone is signed in. It needs administrator rights once, to install.

Runs as	A Windows service (Local System), plus a tray icon for each signed-in user (started for people already signed in when it's installed, and at each sign-in)
Talks to	`installpro.app` over HTTPS, port 443, outbound only
How often	A check-in about every 60 seconds, plus one waiting request (renewed about every 50 seconds) that the console answers as soon as a job is ready for that PC; every few seconds for 10 minutes after someone opens the printers page
Listens on	Nothing on the network. The tray icon talks to the service on `127.0.0.1:47231`, which refuses anything not from the same PC
Its files	`C:\Program Files\installpro.app` (the program) and `C:\ProgramData\installpro.app` (settings, key and a log kept under 1 MB)
Its key	Stored in `agent.json`, readable only by Windows and administrators

What it does

1. **Checks in** and reports the PC's name, Windows version, agent version, network addresses, signed-in user names, the printers installpro.app installed, and the name and network address of the PC's other network printers (so an old copy of a copier can be replaced when installing, if the provider chooses).
2. **Installs printers** your provider set up, when someone asks for one (from the PC's printers page, or by the provider from Deploy). It unpacks the driver, adds it to Windows' driver store (`pnputil`, `Add-PrinterDriver`), adds a Standard TCP/IP port to the printer's address and adds the printer, then applies the provider's default settings (for example black and white, or double-sided).
3. **Updates printers** it installed when your provider changes one (its name, address, driver or defaults) and asks PCs to update, or when someone clicks Update or Reinstall on the PC's printers page. It's the same install again, in place; a renamed printer's old name is removed first.
4. **Removes printers** it installed, when asked.
5. **Opens a printer's settings window**, only when your provider asks for it from Deploy and only for a printer installpro.app installed on that PC. A small installpro.app window appears for the person signed in, who can open the driver's own Printing Preferences, choose the defaults and click OK, or close it. Only the settings chosen there are sent to installpro.app; nothing else on the PC is read. Those settings are then applied as the printer's defaults when it's installed on other PCs. On a PC at the provider's own office (one a provider staff member has marked as their own), the provider can do this for a printer that isn't installed there: the agent adds a temporary copy of the printer with its driver, pointed at no reachable device and used only to show the window, and removes it straight afterwards. Nothing is printed and nothing is sent to the customer's copier.
6. **Looks for copiers and printers** on the network once a day (section 4).
7. **Updates itself** when a new version is released: at a quiet time (overnight, 1 to 5 AM on the PC's clock, or while nobody is signed in to the PC), never in the middle of installing a printer, or straight away if your provider clicks Update.

What it doesn't do: read or keep documents, print jobs, files, browsing, email or keystrokes; take screenshots or remote control; run commands that installpro.app sends as text; or open any port to the internet. The only things your provider can ask a PC to do besides printers are two fixed network checks: **ping** an office address (192.168.x.x, 10.x.x.x or 172.16-31.x.x, never the internet), and show the PC's **network settings** (addresses, gateway, DNS, MAC), much like `ipconfig /all`.

Driver signatures. When a printer driver's catalog carries a valid signature from its maker (for example Kyocera), the agent adds that maker's certificate to the PC's **Trusted Publishers**, so Windows installs the driver without a prompt. Drivers come only from your provider's driver library or installpro.app's own.

Updates are downloaded from installpro.app over HTTPS and installed only if their SHA-256 fingerprint matches the one installpro.app announced. The previous version is kept so an update that fails is rolled back.

Removing it. The agent appears in Windows' **Apps** list with an Uninstall button. Your provider can also uninstall it from Deploy. Uninstalling removes the service, the tray icon, the program folder and the PC's key, and tells installpro.app the PC has left. Only the log in `C:\ProgramData\installpro.app` stays, and can be deleted.

4. Finding copiers and printers on the network

Once a day, one PC per office looks for copiers and printers, so your provider can see their toner and page counts (in installpro.app Monitor, or Deploy). Your provider can also ask for a look straight away ("Scan now"), and can download the list of devices as an Excel or CSV file; only your provider's team sees it.

Where it looks: the PC's own office networks (private addresses only; a large network is limited to the 1,024 addresses around the PC). Your provider can add other office networks, such as a wired network when PCs are on Wi-Fi, up to 4,096 addresses. The agent refuses any address that isn't a private office address (10.x, 172.16–31.x, 192.168.x), even if asked.

STEP	HOW	PORT
Find	Bonjour (mDNS) question for printing services	UDP 5353, local network only
Find	WS-Discovery probe for print devices (as Windows does)	UDP 3702, local network only
Find	A connection attempt to the common printing ports on each address, closed straight away	TCP 9100, 631, 515
Read	SNMP read-only questions (v2c, then v1), community `public`	UDP 161

What it reads from each copier or printer: its make, model, serial number, name, toner levels and page counts (total, and black and white versus color for brands that report them). It sends

nothing to devices except these read-only questions, and changes no device settings.

The whole look is gentle: a few small packets per address, taking a minute or two. If your security tools flag port checks or SNMP, they can be allowed for the scanning PC.

Copier tags. Your provider can print a tag for each new copier, to tape on it for delivery. Its QR code holds a long random code for that one copier. Scanning it opens a page, with no sign-in, that shows only the copier's model, serial number, ID number and where it goes, plus an **Installed** button that updates your provider's records. It shows no contact details, network settings or passwords, and stops working once the install is finished. Passwords are never printed on a tag.

A monitor box instead of a PC: for an office with no PC to use, your provider may plug in a small Linux computer (a "monitor box") that does only this: it finds copiers and printers and reads their toner and page counts, the same way and on the same ports. It installs no printers. Like the agent, it only connects out to installpro.app over HTTPS, and it runs as a system service. It updates itself: it downloads the new version over HTTPS, checks its SHA-256 against the one installpro.app gives, checks that it runs, keeps the old one, and then restarts.

Ready-made boxes: a box can come from your provider unclaimed, with its own code on a label (like BOX-7KQ2X4). Your provider joins it to your office by typing that code in installpro.app; a code works only for the one box that made it. Until it's joined, the box also shows a small setup page on your network (http://installpro-box.local), where an activation code can join it. That page only accepts a real activation code, refuses to be posted to from other websites, allows 5 wrong codes per 15 minutes, closes the moment the box is joined, and closes by itself a few hours after the box starts if nobody uses it. A joined box has no web page at all.

5. Your data

installpro.app keeps only what's needed to set up and look after your printers. Your provider manages your information, and installpro.app handles it on their behalf.

KIND	WHAT'S KEPT	WHERE IT COMES FROM
Your organization	Name, contact name, email, phone, address, office locations, notes	Your provider
People who sign in	Name, email, role; passwords only as a scrambled bcrypt hash	Your provider, or you when invited

KIND	WHAT'S KEPT	WHERE IT COMES FROM
PCs	Computer name, Windows version, agent version, network addresses, signed-in Windows user names, installpro.app printers on it, last check-in	The agent
Installations (Workflow)	Target install date and schedule, the provider's people assigned, each copier's make, model, location, serial number, ID number, network address and progress, checklist answers (including a staff list of names and emails for printer sign-ins, if you give one), notes, files and install-day photos	Your provider, and you on your checklist page
Scan history (Monitor)	The last 60 scans at each office: when, which box or PC, the network looked on, how many addresses answered, and the names and IP addresses of copiers and printers that were new or missing. No other devices on the network are listed, only counts. Only the provider's team sees it.	Your provider's team only
Alerts (Monitor)	When the provider's monitor box, an important PC or a copier stopped checking in or being seen, and when it came back. Built from the check-ins and scans above; nothing new is collected from your PCs	Your provider's team only
Build sheets (Workflow)	The provider's internal form for an install: each copier's accessories, toners, apps and licenses, serial numbers, activation keys (encrypted like saved passwords), meter readings and a build checklist	Your provider's team only
Saved passwords (Workflow)	Logins for an install (Wi-Fi, scan-to-email and the like), encrypted with a key that's only on our server. Only the provider's team can show one, and every time is recorded.	Your provider, or you on your checklist page
Address books (Convert)	Only address books the provider saves: names, emails, fax numbers and scan-to-folder locations. Never passwords (removed before saving).	Until the provider deletes it
Printers	Name, network address, model, serial number, driver, default settings (including settings saved from the driver's own window, which can hold a department or account code)	Your provider
Copiers found on the network	Address, make, model, serial number, toner levels, page counts (one reading a day kept for monthly volume); the provider's ID number and whether they look after it	The agent; the provider (in Monitor)

KIND	WHAT'S KEPT	WHERE IT COMES FROM
Support	Messages and screenshots sent to your provider or to installpro.app	You or your provider

Never collected: documents or anything printed, print job contents, files, browsing, email, keystrokes, screenshots of PCs, or payment card details.

Where it's kept: in the United States, on a DigitalOcean server; uploaded files (drivers, screenshots) and backups in Cloudflare R2. Emails are sent through Resend.

How long: until your provider deletes it. Deleting a customer deletes its offices, installations, printers, PCs, accounts and support messages. A copy of the database is backed up each night and kept up to 30 days, so deleted information leaves the backups within 30 days. Backups are restore-tested.

The full privacy policy has the details, including how to ask for a copy of your information or for it to be deleted.

6. Security controls

AREA	CONTROL
Connections	HTTPS everywhere, with certificates renewed automatically. Browsers are told to use HTTPS only (HSTS).
Separation	Each provider sees only its own customers, and each of your people only your organization. A test with one provider's admin trying 25 of another provider's pages and actions found every one refused.
Roles	Super Admin, Admin and Tech at the provider; Client for your own staff. Clients see only your printers and how to set up a PC.
Apps	One account signs in to every app (Workflow, Deploy, Convert). Each provider sees only the apps installpro.app has turned on for them.
Passwords	At least 10 characters, stored as bcrypt hashes. Repeated wrong passwords, activation codes or reset requests are slowed down after 10 tries.
Sign-ins	Random 32-byte session keys, stored hashed, in cookies scripts can't read. Signed out when the browser closes or after 8 hours unused, unless someone ticks "Keep me signed in" (14 days). Changing a password signs out every other browser.
Password links	Single use; expire in 1 hour (7 days for a welcome email).

AREA	CONTROL
Checklist links	No account needed: a random secret in the link, stored hashed. Each person gets their own; they work for 30 days and the provider can switch any of them off.
Activation keys	On a provider's build sheet: the same AES-256-GCM encryption as saved passwords. Shown only to the provider's team, on the sheet and its printout. They're never in the text of an email. With **Email as PDF**, a team member can send the build sheet as a PDF attachment (no link) to people on their team or to any email address they type, up to 10 at a time. Keys are left out of that PDF unless they tick **Include activation keys** (off each time), and even then only the copies to people on their own team have keys; typed-in addresses always get a copy without them. The PDF does carry the customer's name, address and contact, and the copiers' serial numbers, so it's the sender's choice who gets it.
Saved passwords	AES-256-GCM encryption, with the key kept in the server's settings, not in the database or its backups. Shown only to the provider's team, logged, never printed, and never shown back to the person who typed it.
Web protections	Forms from other sites are refused; pages can't be shown inside another site; pages aren't kept in the browser's cache.
PC keys	A unique key per PC, stored hashed by installpro.app. Removing a PC in Deploy stops its key working at once.
Activation codes	12 random characters; your provider can replace yours at any time. PCs that already joined keep working.
Uploads	Size and file-count limits; files with unsafe names refused. Screenshots are shown with strict browser rules.
Provider support access	The installpro.app owner can view a provider's apps to help, look-only unless switched to making changes, and the provider can see each visit.
Server	Only HTTPS and key-based SSH are open; the application isn't reachable directly; security updates install automatically.
Availability	Checked every 5 minutes by an outside monitor, including the database.

Code signing. Signing the agent with a code-signing certificate is under way. Until then, Windows may show "Unknown publisher" when the setup runs.

7. Checklist for IT

Firewall and filtering

- [ ] Allow PCs to reach `https://installpro.app` (TCP 443, outbound). Nothing inbound is needed.

- [ ] On the PC that scans each office: allow outbound TCP 9100, 631 and 515 and UDP 161 to the printers' networks, and UDP 5353 and 3702 on the local network. Without these, printing still works; only the toner and page counts are missing.
- [ ] If web traffic must pass through a proxy, tell your provider before rollout: the agent connects directly today.
- [ ] If your security software holds new programs for review, allow `installpro-agent.exe` from `C:\Program Files\installpro.app`.

Deploying

- [ ] **A few PCs:** open the setup link your provider sends on each PC and click Yes when Windows asks. The PC joins your organization by itself.
- [ ] **Many PCs (Group Policy, Intune, RMM tools):** use the **MSI** your provider gives you (signed, like the agent) and install it silently: `msiexec /i installpro-setup-<code>.msi CODE=<your activation code> /qn`. It runs the agent's own installer, so updates and removal work as described here, and only one installpro.app entry appears in Apps. Or push `installpro-agent.exe` and run it silently as administrator: `installpro-agent.exe install --code <your activation code>`.
- [ ] Check the PCs appear as online in your provider's Deploy (or ask your provider).

Removing

- [ ] Windows Settings, Apps, **installpro.app**, Uninstall; or ask your provider to uninstall it from Deploy; or run `installpro-agent.exe uninstall --forget` as administrator; or, if it was installed with the MSI, `msiexec /x installpro-setup-<code>.msi /qn`.

8. Questions IT often asks

Can installpro.app, or our provider, control our PCs? No. The agent only installs and removes the printers your provider set up, and reads copiers' status. There is no remote desktop, file access or command line. Your provider can run two fixed network checks (ping an office address, or see a PC's network settings) to find out why a copier isn't reachable.

Do users need administrator rights to add a printer? No. The service installs the printer for them when they pick it from the printers page.

What if installpro.app is down? Printers already installed keep printing: print jobs go straight from the PC to the printer, never through installpro.app. Only adding or removing printers waits until it's back.

Does printing go through the cloud? No. installpro.app sets up a normal Windows printer that prints directly to the copier on your network.

What happens if a PC is lost or replaced? Your provider removes it in Deploy, and its key stops working at once.

Can we see what the agent did? Yes: `C:\ProgramData\installpro.app\agent.log` on each PC, and your provider's Deploy lists every install and removal.

Who do we contact? Your provider first, since they manage your printers. For installpro.app itself: support@installpro.app.

© 2026 installpro.app · Console 1.0.42 · Agent 0.10.5