Secomea vs. Privileged access management (PAM)

Protecting privileged identities and securing industrial access are different jobs.



PAM governs privileged access. OT also needs control down to the machine.

PAM is essential for protecting privileged accounts, credentials, administrative access, and elevated activity across enterprise systems.

Some PAM platforms also support third-party and OT access. But their operating models are typically centered on identities, credentials, and administrative systems rather than frequent access to individual industrial machines.

An OEM engineer troubleshooting a PLC creates a different access problem.

You must be able to manage, control, and audit **which plant, which machine, which services, for how long, who locally approves the work, and how the complete session is documented.**

Secomea is purpose-built around those operational OT requirements.

WHY SECOMEA WINS FOR OPERATIONAL OT ACCESS

Govern the machine – not only the privilege

Secomea controls access around the user, machine, service, site, session, and approved period.

That gives OT the asset-level precision required for industrial service.

Let the plant manage the service event

OT can approve planned or urgent vendor access within security boundaries established by IT.

IT retains governance and auditability. OT keeps operations moving.

Give external users only what the job requires

Each vendor, OEM, contractor, or service partner can have an individual identity and time-limited permissions to specific industrial assets and services.

Built around industrial systems and workflows

Industrial protocols, engineering applications, legacy equipment, and agentless assets are part of Secomea's operating model – rather than exceptions that have to be fitted into a broader enterprise-access workflow.

WHICH ACCESS PROBLEM ARE YOU SOLVING?

	PAM	Secomea
Primary function	Protect privileged identities and administrative access	Secure remote interaction with industrial assets
Primary control object	Accounts, credentials, privileges, commands	Users, machines, services, sessions, time
Typical users	Administrators and privileged enterprise users	OT, engineers, OEMs, vendors, service partners
Typical targets	Servers, applications, databases	PLCs, HMIs, SCADA, controllers, industrial equipment
Daily ownership	IT- or security-led	OT-led, IT-approved
Best fit	Enterprise privileged-access risk	Frequent or time-critical OT remote access

THE DECISION

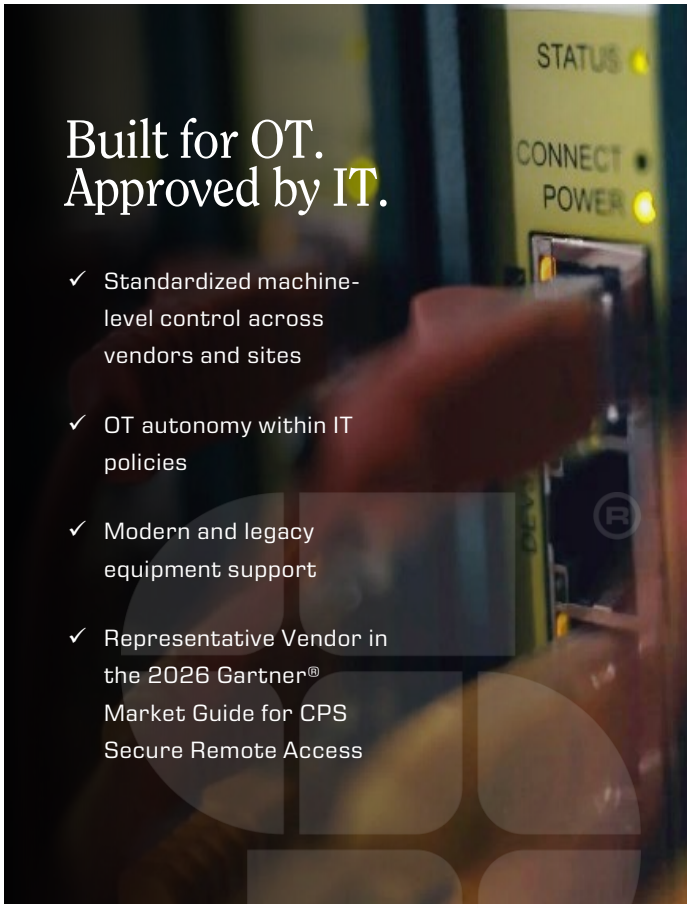
Choose PAM when your main requirement is protecting privileged accounts, credentials, and administrative activity across the enterprise.

Choose Secomea when the business problem is giving vendors and engineers secure, precise access to industrial equipment without turning every intervention into an IT-admin workflow.

***Already have PAM?* Keep it for the job it does well.**

Secomea can provide the dedicated OT access layer alongside that enterprise governance.

PAM protects privilege. Secomea makes secure industrial access operational.



Built for OT. Approved by IT.

- ✓ Standardized machine-level control across vendors and sites
- ✓ OT autonomy within IT policies
- ✓ Modern and legacy equipment support
- ✓ Representative Vendor in the 2026 Gartner® Market Guide for CPS Secure Remote Access

Put your PAM workflow against a real OT intervention

Take an actual scenario: an external engineer, a mission-critical machine, and a limited maintenance window.

We will show you what changes when remote access is designed around the machine and the work – not only the privileged identity.

Compare Secomea with your PAM approach →

Category descriptions are general. Individual platform capabilities, architectures, and configurations may vary.