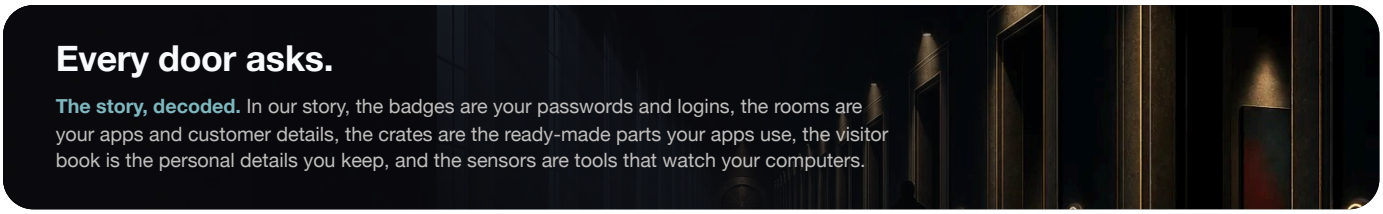
ALGOSHRED TECHNOLOGIES

SECURITY & TRUST · EVERY DOOR ASKS

One check at the front isn’t enough.

Security and trust engineering means your systems check who is asking, what they’re allowed to touch and whether it’s still the right time, at each door, instead of trusting anyone who got past the front door.



Every door asks.

The story, decoded. In our story, the badges are your passwords and logins, the rooms are your apps and customer details, the crates are the ready-made parts your apps use, the visitor book is the personal details you keep, and the sensors are tools that watch your computers.

SOUNDS FAMILIAR?

- Once someone’s logged in, they can see pretty much everything.
- People who left last year still have a login somewhere.
- One shared password opens the money side of things.
- Security checks happen at the end, if someone remembers.

THE IDEA IN PLAIN WORDS

Every door asks, not just the front one

Each room checks who’s asking, whether they’re allowed in, and whether it’s still their shift, so one stolen badge reaches much less of the building.

Experts file this under: zero trust, segmentation

Worth knowing
No setup makes a break-in impossible. Checks at every door make one harder to pull off and easier to spot. “Zero trust” is a way of working, not a product you buy.

Badges for tonight, for the rooms the job needs

People and apps get only the rooms their work needs, only while they need them, with a second proof at the risky doors, and old badges are taken back.

Experts file this under: identity and access management, least privilege, just-in-time access, two-step sign-in

Worth knowing
Tighter badges mean a few more asks at the risky doors, so we keep the everyday doors easy.

Locks drawn into the plans, checks on everyday changes

Ask how a burglar would get in before you build, add quiet checks to everyday changes, then test the finished building the way a curious burglar would.

Experts file this under: security by design, DevSecOps, application security testing

Worth knowing
Checks and tests catch many weak spots, not all of them.

Check the crates, keep less in the visitor book

Know which outside parts come in and who sent them, and collect only the personal details you need, shown only to the people who need them.

Experts file this under: software supply-chain security, privacy by design

Worth knowing
Dock checks catch many bad crates, not all, and a known sender isn’t enough on its own. Packing lists are kept and re-checked. Laws differ by country, so we work with your legal advisers. Nothing here is legal advice.

HOW WE WORK WITH YOU

STEP 01
Walk
Which doors matter most, who holds which badges, which crates come in, what goes in the visitor book.

STEP 02
Map
Mark the open doors and the old badges, and agree a short list of what to fix first and why.

STEP 03
Lock
Tighten the riskiest doors and badges with your teams, one system at a time.

STEP 04
Build in
Quiet checks become part of everyday changes.

STEP 05
Watch & teach
Sort what the sensors see, write and try the calm plan, and coach your people to run it.

Start small: a walk-through of one app or system, a badge clean-up, or a dock check of one app’s outside parts.

WHAT WE HELP WITH

Keys held by apps, scripts and AI helpers
Fewer forgotten keys lying around, each with a name and an owner.

Test the finished building like a curious burglar
Weak spots found in a test rather than in a break-in, with a plain list of what to fix first.

Collect less, show less, keep it tidy
Less to lose, and plainer answers when customers ask what you hold.

Spot the one odd thing, and respond calmly
Odd things are easier to spot, and a bad night follows a plan.

Do your doors ask?

Start with one door: email contact@algoshred.com with the system or data you worry about most, and we’ll suggest a first step.

Vignesh T.V., CEO & CTO, Algoshred Technologies Pvt. Ltd.

WATCH THE FILM
algoshred.com/security-trust