ALGOSHRED TECHNOLOGIES

SECURITY & TRUST · EVERY DOOR ASKS

One check at the front isn’t enough.

We help every door of your apps and data ask who’s there, give people and apps only the badges their work needs for as long as they need them, and build the checks into the way your teams already work.

Worth knowing: No setup makes a break-in impossible. Checks at every door make one harder to pull off and easier to spot. It’s step by step, starting with the doors that matter most.

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

Security & trust engineering as a service

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

contact@algoshred.com

The problem, and the idea.

- 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.
- Nobody's sure which outside parts our apps are built from.
- We collect personal details 'just in case', and keep them for good.

> **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.**

The story, decoded. In our short film, the museum is your business's systems, the rooms are your apps and customer details, the badges are passwords and logins (so Mira's stolen badge is a stolen password), 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. Master keys are admin logins; the locked cabinet, a password vault.

01 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.

02 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.

03 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.

04 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.

One stolen badge: one check at the front, or every door asks.

ROOM	ONE CHECK AT THE FRONT	EVERY DOOR ASKS
Front desk	The guard scans the badge. It's real, so the reader says yes.	The guard scans the badge. It's real, so the reader says yes. That's the first door, not the last.
Lobby	Open, like every room past the desk.	Open to visitors, like your public website, so it doesn't ask. Nothing valuable sits here.
Paintings gallery	Open. Nobody asks again.	✕ **said no** Asks who you are and whether it's still your shift. Mira works days, so the door says no. `Paintings door: asked, said no, noted.`
Staff office	Open, with the staff files on the desk.	✕ **said no** Asks whether it's still your shift. Mira's shift ended hours ago, so the door says no. `Office door: asked, said no, noted.`
Archive	Open. Anything inside can walk out.	✕ **said no** Asks whether this badge is allowed in here. A restorer's isn't, so it says no. `Archive door: asked, said no, noted.`
Vault	Wide open, propped with a mop. A painting leaves under an arm.	✕ **said no** Wants two proofs: the badge and a code sent to Mira's phone. The thief has only the badge. `Vault: asked for a second proof, said no, noted.`

In your business: one stolen password, and how far it reaches. An illustration, not a measurement.

Make a badge for tonight. In your business: each login opens only what that job needs, for as long as it's needed.

THE CLEANER
- Lobby
- Paintings gallery
- Broom cupboard

Opens the paintings gallery and the broom cupboard. Not the vault.

THE RESTORER
- Lobby
- Paintings gallery
- Staff office
- Restoration studio

Opens the rooms a restorer works in, by day. Not the archive or the vault.

A DELIVERY DRIVER
- Loading dock

THE NIGHT MANAGER
- Lobby
- Paintings gallery
- Staff office
- Archive
- Vault (second proof)

Even the night manager's badge asks for a second proof at the vault.

THE NIGHT-LIGHT ROBOT THAT RUNS ITSELF
- Gallery light switches

Apps, scripts and AI helpers carry badges too.

Badge for tonight: Stops working at closing. **Badge for good:** Keeps working after the job is done. The vault asks for two proofs, like a password and a code on a phone. **The drawer of old badges:** Old badges nobody took back still work, so a routine takes them back.

Who sent this one? In your business: the outside parts, add-ons and downloads your apps are built from.

CRATE	IT CAME FROM WHO IT SAYS	THE SEAL IS UNBROKEN	THE NAME IS REALLY THE ONE YOU ORDERED	WHAT'S INSIDE MATCHES THE PACKING LIST	AT THE DOCK
From a sender we know, seal whole	• **checks out**	• **checks out**	• **checks out**	• **checks out**	In it goes, and its packing list is kept on file.
From a sender we know, seal torn	• **checks out**	✕ **doesn't match**	– not checked	– not checked	Set aside, unopened, to check again. A known sender isn't enough on its own.
Stencilled "From: not a thief"	✕ **doesn't match**	– not checked	– not checked	– not checked	Wheeled straight back out the gate, unopened.
Lookalike name: "Galery lights" (we ordered Gallery lights)	• **checks out**	• **checks out**	✕ **doesn't match**	– not checked	Close, not close enough. Sent back.

Later, a sender says one part needs a fix: The packing lists show which galleries hold that part, so it can be fixed where it is.

Worth knowing
No setup makes a break-in impossible. Checks at every door make one harder to pull off and easier to spot.

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

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.

What we help with.

Start with the door that worries you most, or bring the pieces together, one system at a time.

Make every door ask

We find which rooms matter most, put walls between them and make each door check who is asking, from where and on what device, starting with the riskiest.

A stolen badge reaches less of the building.

> **Experts file this under: zero trust architecture, segmentation, access without a VPN**

Right badges, for the right time

One sign-in for staff, a second proof at the risky doors, master keys (admin logins) signed out for a task and returned, and a routine that takes badges back when people leave or change roles. Password resets at the help desk get a proper check too.

A stolen password alone opens less, and old badges are taken back on a routine.

> **Experts file this under: identity and access management, single sign-on, two-step sign-in, passkeys, privileged and just-in-time access, access reviews**

Keys held by apps, scripts and AI helpers

Count the passwords and keys your apps, scripts and AI helpers carry, move them out of the code into a locked cabinet (a password vault for apps), give each one an owner, and change them on a routine.

Fewer forgotten keys lying around, each with a name and an owner.

> **Experts file this under: machine identities, secrets management, secret scanning, agent identity**

Draw the locks into the plans

Ask “how would a burglar get in?” before building, and add quiet, well-tuned checks to everyday changes, so teams fix things while the work is fresh.

Problems show up earlier, while they are small.

> **Experts file this under: threat modelling, DevSecOps, security checks in the delivery pipeline, policy as code**

Test the finished building like a curious burglar

Hands-on testing of your apps and the doors between them, including the parts that talk to AI models, with plain write-ups of what to fix first.

Weak spots found in a test rather than in a break-in, with a plain list of what to fix first.

> **Experts file this under: application security testing, code review, penetration testing, API and AI-app security**

Check the crates at the dock

A packing list for each app’s outside parts, checks on the seal and the sender, a watch for lookalike names, and a routine to hear when a part needs a fix.

You have a list of what your software is built from, and where each part came from where it can be traced.

> **Experts file this under: software supply-chain security, SBOM, signing, provenance, SLSA, dependency scanning**

Collect less, show less, keep it tidy

Find where personal details live, collect only what has a stated purpose, show each person only what they need, and delete on schedule or on request.

Less to lose, and plainer answers when customers ask what you hold.

> **Experts file this under: privacy engineering, privacy by design, data minimisation, retention**

Spot the one odd thing, and respond calmly

Sensors on your computers and accounts notice odd sign-ins; we sort what they see so the odd thing stands out, write a calm plan with your team (close the door, call the right people, write it down) and try the plan out together.

Odd things are easier to spot, and a bad night follows a plan.

> **Experts file this under: security operations, detection and response, incident response, tabletop exercises**

We start from whatever you already use, for example your cloud provider’s sign-in and key services, sign-in services (such as Microsoft Entra ID, Okta or Google), password vaults for apps (such as HashiCorp Vault), tools that seal software parts (such as Sigstore), code and parts scanners, and your log and alert systems.

Capabilities, from the front door to the night watch.

From who holds which badge, to locks drawn into the plans, to checking the crates at the dock, to a calm plan for an odd night.

Doors and badges

Who can open which door, and for how long.

- Access that asks at every door, with walls between systems
- Sign-in, second proofs, and passkeys (signing in with your phone or fingerprint instead of a password)
- Routines for people joining, moving and leaving, with regular checks of who has access
- Master keys signed out for a task, and returned
- Keys held by apps, scripts and AI helpers

Built in, not bolted on

Locks in the plans, and quiet checks on everyday changes.

- Threat modelling before building: how would a burglar get in?
- Well-tuned checks on everyday changes
- House rules the computer checks (policy as code)
- Hands-on testing of apps, the connections between them, and AI features

What comes in, what you keep

Know your crates, and keep the visitor book short.

- Packing lists for software parts (SBOM)
- Seals, sender checks, and guarded steps where your apps are built and packaged
- Collect only the personal details you need, and show them only to who needs them
- Routines to delete personal details on time

The night watch

Notice the odd thing, and know what to do next.

- Sign-in and activity logging that shows what matters
- Calm response plans, and practice runs with your team
- Evidence gathered as you go, for customers, auditors and regulators
- Coaching, and a named go-to person for security questions in each of your teams

WHERE IT BECOMES REAL · ILLUSTRATIVE EXAMPLES

Retail and e-commerce

A support agent's leaked password opens the order screen it was made for, not the payment settings, and a second proof guards refunds and account changes.

Financial services

Money-moving systems ask for a second proof, master keys are signed out for the task and returned, and the record of who did what is kept as evidence.

SaaS and product companies

New features go through the same quiet checks, and each release carries a packing list of its outside parts, ready for when a customer asks to see it.

Healthcare

Reception staff see the appointment, not the diagnosis; patient details are shown on a need-to-know basis and deleted on schedule.

Manufacturing and connected products

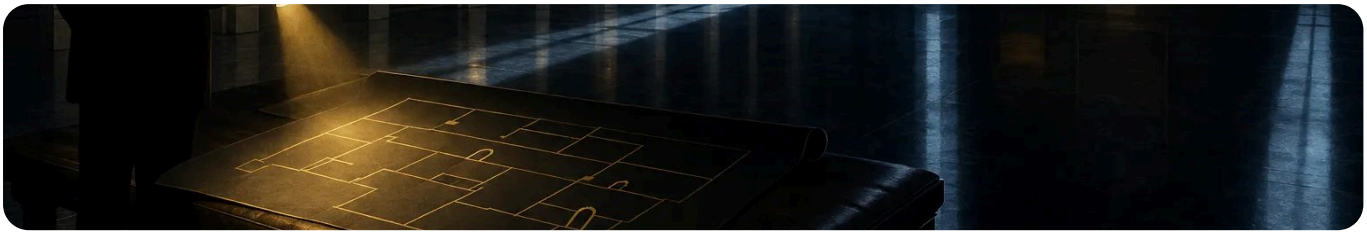
Devices and the software inside them carry sealed parts and a packing list, so a part that needs a fix can be found across product lines. Some countries now ask product makers to keep such lists (rules differ by country; not legal advice).

Teams adopting AI helpers

AI assistants and agents get their own badges with only the rooms they need, their keys live in the locked cabinet, and what they do is logged like anyone else's.

HOW WE WORK

Walk the building first, then lock the riskiest doors.



01 WALK

Walk the building with you

We walk the building with you: which doors matter most, who holds which badges, which crates come in and what goes in the visitor book. We talk to the people who run each system, not only to the plans.

02 MAP

Draw the doors that matter

We mark the open doors and the old badges on one map, against a checklist or standard you already follow (if any). Then we agree with you a short list of what to fix first, and why.

03 LOCK

Lock the riskiest doors first

We tighten the riskiest doors and badges with your teams, usually starting with sign-ins and who holds which keys, one system at a time.

04 BUILD IN

Put the checks into everyday work

We add quiet, well-tuned checks to the way your teams already work, so changes, crates and new features go through the same checks. Problems show up while the work is still fresh. Checks and tests catch many weak spots, not all of them.

05 WATCH & TEACH

Watch, and teach your team

We help sort what the sensors see so the odd thing stands out, write a calm response plan with your team and try it out together, and coach your people to run it. We can stay on to help with the next doors if you prefer.

Ways to start

A walk-through of one door. One app or system, who holds its badges, and the crates it takes in.

Badge clean-up. Who has which keys, which old ones to take back, and where a second proof belongs.

Dock check. A packing list of the outside parts in one app, and a routine to keep it fresh.

What you get

- A map of the doors that matter, and who holds which badge
- A short list of what to fix first, and why
- Checks added to how your team builds and releases changes
- A packing list for each app's outside parts
- A calm response plan, tried out with your team
- Notes and coaching for the people who will run it

NEXT STEP

Questions, myths and the next step.

What does “zero trust” actually mean?

Nobody is trusted just for being inside. Every door checks who is asking, what they’re allowed to touch and for how long. “Zero trust” is a way of working, not a product you buy.

Will this slow my team down?

The checks run inside normal work, so people aren’t tempted to prop doors open. Tighter badges mean a few more asks at the risky doors, so we keep the everyday doors easy.

Where do we start?

With the door that matters most, usually sign-ins and who holds which keys. A badge clean-up and a second proof at the risky doors are often the smallest useful first steps.

Do we have to replace our tools?

Not usually. We start with what you already have, and add only where it helps.

We’re small. Is this for us?

Yes. Automated attacks try lots of doors at once; they don’t check your size first. The smallest useful version is short: take back old badges, add a second proof where money or customer details live, and keep a list of the outside parts your apps use.

Can you help with audits and regulations?

We help you gather the evidence your auditors, customers and regulators ask for as you go, and explain the gaps in plain words. We don’t promise an audit result. Laws differ by country, so we work with your legal advisers. Nothing here is legal advice.

What about the parts of our apps we didn’t write?

We make a packing list of them, check the seal and the sender where we can, and set up a routine so you hear when one needs a fix. 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.

What happens after the project ends?

Your team keeps the maps, the checks, the packing lists and the calm response plan, and we coach them to run it. We can stay on to help with the next doors if you prefer.

MYTHS, ANSWERED

“We have a strong front door, so we’re fine.”

A real badge in the wrong hands walks straight past a front door that only checks badges, and past it nothing asks again. Every door needs to ask.

“We’re too small to be a target.”

Automated attacks try lots of doors at once. They don’t check your size first.

“Our cloud company looks after all of it.”

They look after the walls and the wiring. You still decide who gets keys to your rooms, and what’s left lying on the table.

“Security is a product you buy once.”

It’s mostly habits and checks: badges reviewed, locks tested, crates checked. Tools help. “Zero trust” is a way of working, not a product you buy.

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.

contact@algoshred.com

WATCH THE FILM

algoshred.com/security-trust