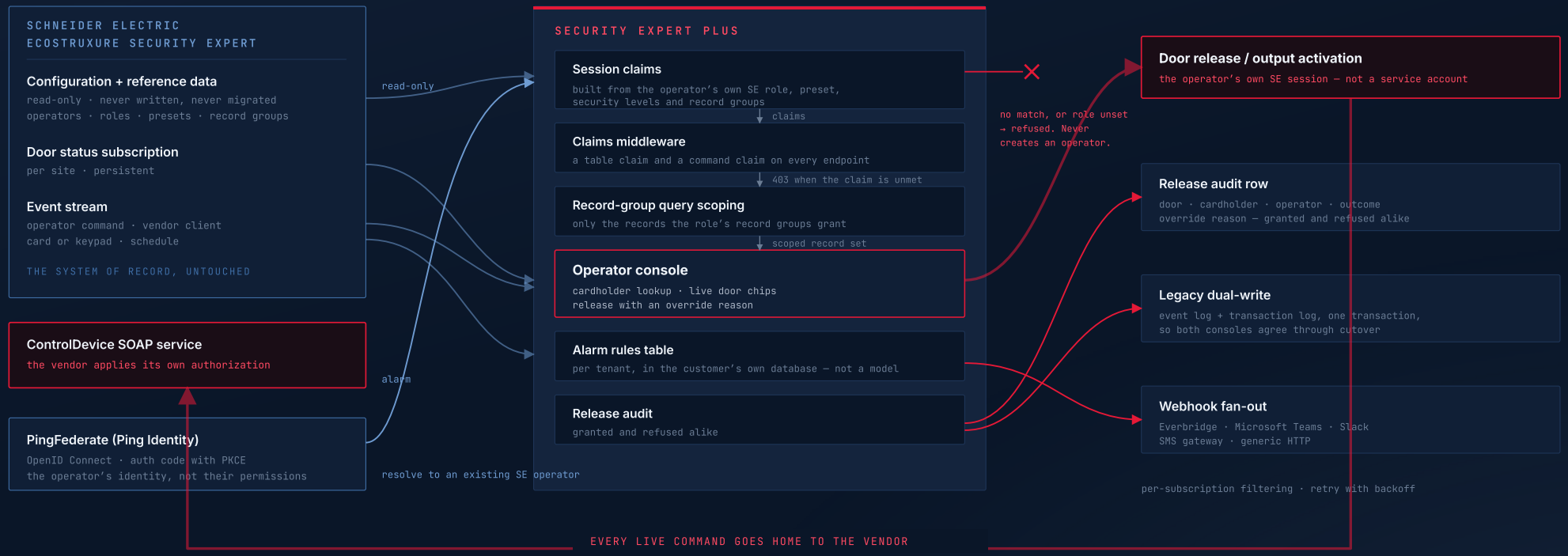
OPERATIONS LAYER

Security Expert still decides.
SX+ decides who asks.

Security Expert Plus is Knight Watch's independent operations platform, built to run on top of **Schneider Electric EcoStruxure Security Expert**. It enforces Security Expert's own permission model rather than replacing it: the vendor's configuration becomes the session's claims, and every live control command still goes back through Security Expert's own SOAP service — under the signed-in operator's session, not a shared service account.



Not yet formally released to production — no production go-live is evidenced as of 31 August 2026. The operator console is built and code-complete with automated test coverage; every other capability on this deck carries its own status on the board where it appears.

OPERATOR CONSOLE

Find the person, open the door, say why.

The operator console is the one screen a guard works from — a module inside Security Expert Plus. Individual engagements deploy it under customer-chosen names; those names are not used in Knight Watch marketing. Its tabs follow the operator's access claims, **enforced server-side rather than in the browser**, and the same claim check runs on every endpoint behind them.

Cardholder lookup

Search the Security Expert cardholder records the operator is actually scoped to see, with the cardholder photo served from its own database rather than copied into the console's.

- → Only the records the operator's record groups grant
- → Photo retrieved on demand, per cardholder
- → Read-only against vendor-owned data

Door release, with a reason

Every door release that bypasses an access-level or state rule requires an explicit human acknowledgement with a written reason, and that reason is recorded against the access-control event in a dedicated release-audit table.

- → Override acknowledgement is mandatory, not dismissible
- → The written reason is stored with the release, not typed into a chat
- → Refusals are captured with the same detail as releases

Live door state

Door chips on the console update live: a lock, unlock, or latch shows immediately whether it came from an operator command, the vendor's own client, a card or keypad swipe, or a scheduled action.

- → An operator command
- → The vendor's own client
- → A card or keypad swipe
- → A scheduled action

Built and code-complete with automated test coverage; formal customer acceptance testing has not yet taken place. The tab list is the build as of 31 August 2026 and will change.

PERMISSION MODEL

No Security Expert operator, no session.

SINGLE SIGN-ON	the operator console includes a PingFederate (Ping Identity) OpenID Connect sign-in path — Authorization Code with PKCE — that resolves the federated identity to an existing Security Expert operator.
FAILS CLOSED ON NO MATCH	A user who authenticates successfully at the identity provider but has not been provisioned as a Security Expert operator is denied access, and the SSO sign-in flow never creates an operator account.
THE UNSET-ROLE GATE	the operator console refuses a session to any operator whose role in Schneider Electric Security Expert is left unset. An unprovisioned account is denied at sign-in rather than admitted with an empty permission set — and where single sign-on is deployed, the same gate is applied at identity resolution, so an operator refused one sign-in route cannot enter by the other.
CLAIMS, CHECKED SERVER-SIDE	Role, Preset, Security Levels and Record Groups become the session's claims. A server-side claims middleware checks the required table and command claim on every authenticated API endpoint and returns 403 when it is not met, and every live control command still goes through the Security Expert SOAP service, which applies its own authorization.

KNIGHT WATCH

RECORD-GROUP SCOPING — VERIFIED END TO END

Verified end-to-end on a real, narrowly-scoped operator role against a live enterprise estate (12 August 2026): that operator saw only the doors and record groups their role's record groups actually grant, and nothing outside them.

A live OIDC sign-in round-trip was completed in a non-production environment in June 2026; production verification, cutover and group-to-role mapping are pending. The record-group verification is dated 2026-08-12 and is not claimed system-wide.

ALARM PIPELINE

A rules table, not a model.

NO MODEL IN THE LOOP

There is no AI component in this pipeline, and we would rather say so than imply one. Classification is a table the customer owns, in the customer's own database, and every routing decision can be read back out of it. When an alarm goes to the wrong place at 03:00, the answer is a row someone can look at — not a prompt someone has to reconstruct.

The Everbridge channel is built pending live-tenant certification — tenant credentials and payload validation are still outstanding, so it is not yet a live integration. Nothing on this board is claimed to be running in production.

RELEASE AUDIT

Every refusal is audited, not just every release.

Every door-release decision — granted or refused — writes a row to the release audit table. Below is **the schema of that record**, field by field. It is deliberately not a sample of traffic: there is no illustrative data anywhere on this deck.

DOOR — ILLUSTRATIVE SAMPLE

DOOR	WHICH DOOR THE DECISION WAS MADE AGAINST	SCOPED BY THE OPERATOR'S RECORD GROUPS
Cardholder ID	The numeric identifier of the person	This record does not store a card or badge number
Operator	Who made the decision	The same identity the SOAP command is issued under
Timestamp (UTC)	When the decision was made	Written on a grant and on a refusal alike
Outcome	Granted or refused	A refusal is a row, not a silence
Failure reason	Why a refused release was blocked	Badge state hold · no access rights · missing override acknowledgement · operator self-release · controller rejection
Override applied + reason	Whether a rule was bypassed, and the written justification	An override cannot be applied without an explicit human acknowledgement
Event code	The organization's own event codes	The record reads in the customer's vocabulary, not ours

Writing the custom event into Security Expert's own event log, the way the legacy web client did, is a known follow-up and is not shipping today. The fields above are the record's schema, not sample traffic.

STATUS & DELIVERY

Built, verified, and not yet in production.

BUILT AND CODE-COMPLETE

Written and code-complete. The operator console carries automated test coverage; every other item here carries its own status, and several ship from a customer engagement's build rather than the platform mainline.

- Operator console
- Claims middleware — 403 on every endpoint
- Record-group query scoping
- Door release under the operator's own SE session
- Release audit — granted and refused
- Legacy dual-write through cutover
- Per-tenant alarm rules table
- Outbound webhook engine + dispatch history
- Floor plans

Code-complete is not production. No production go-live is evidenced as of 31 August 2026, and formal customer acceptance testing has not yet taken place.

VERIFIED AGAINST REAL CONDITIONS

Tested outside a laboratory, with the date and the environment attached to each result.

- Record-group scoping — 12 Aug 2026, live enterprise estate
- 14 of 14 permission gates correct
- PingFederate OIDC round-trip — June 2026, non-production

SSO production verification, cutover and group-to-role mapping are pending.

BUILT, NOT YET RELEASED

Finished work that has not reached a released build, or that lives on a customer engagement's branch rather than the platform mainline.

- HR read path with circuit breaker — merged 19 Aug 2026
- HID Origo visitor mobile credentials — visitor-only
- Everbridge channel — pending live-tenant certification
- Role-preset fail-open fix — mainline, not the release branch

The HID Origo integration ships disabled by default, targets HID's certification tier, and does not write the issued card number into Security Expert — so the credential alone will not grant at a door until a matching cardholder record exists there.

NOT BUILT TODAY

Named here rather than left for a prospect to find. Badge Requests is hidden from the sidebar for the current engagement milestone — the route stays registered so direct URLs still work — and one of its seventeen scoped items is done.

- Badge photo processing pipeline
- Badge facility / area access audits
- Blacklists
- Console offline local-table failover
- Custom event written into Security Expert's own event log

Roadmap only, zero code today.

A green marker on this deck would mean running in production today — nothing here carries one. Security Expert Plus is pre-release: no production go-live is evidenced as of 31 August 2026, and formal customer acceptance testing has not yet taken place.

HOW YOU RUN IT

Your hosts, your data, your rollback.

Knight Watch publishes a release; your own IT deploys it. There is no standing access into your estate, no data migration, and the console you have today stays available as a fallback the whole way through.

Deploy

Releases are the only deployment artifact. Knight Watch publishes a versioned, checksummed release package; your own IT deploys it to hosts you control.

- → Versioned, checksummed release package
- → Windows / IIS hosts the customer controls
- → Container image also available
- → Production configuration never shipped in or overwritten
- → No Knight Watch access required to deploy

THE DOCUMENTED MODEL — NOT A RECORD OF DEPLOYMENTS PERFORMED

Coexist

Designed to run alongside an existing web client through cutover rather than replace it in one move, dual-writing the legacy audit tables in a single transaction so both consoles agree.

- → Coexists with the legacy web client through cutover
- → No data migration — the same tables, in place
- → Legacy console stays available as a fallback
- → Both consoles see the same audit history

CUTOVER IS A DECISION YOU MAKE, NOT ONE THE INSTALL FORCES

Roll back

Every deployment leaves the previous version on disk, so going back is a documented procedure rather than a restore from backup.

- → Timestamped backup of the previous version, per deployment
- → Documented rollback procedure
- → Legacy client still running throughout
- → Database schema changes ship as a bundled migration

REVERSIBLE BY DESIGN

Support

Business-hours support is standard, with an optional Premium tier adding 24×7 response for critical (P1/P2) incidents.

- → Business-hours support is standard
- → Optional Premium tier: 24x7 for P1/P2
- → Coverage and escalation set by the executed support addendum
- → Emergency patching and deployment automation are separate arrangements

NO UPTIME % OR RESPONSE TARGET IS QUOTED ON A SALES PAGE

No uptime percentage and no response-time target appears on this deck. Those belong to a countersigned support addendum, not to a sales page. Security Expert Plus is pre-release as of 31 August 2026 — see board 06 for what that means item by item.