

Prove your standards are enforced every day, not just on audit day.

Frameworks, controls, policies and evidence — where everything the other two pillars discover turns into something an auditor, a customer or a regulator will accept.

Writing a control description takes an afternoon. Proving it, re-proving it for the next framework, and proving it again at the next audit is what consumes the year. This pillar takes the live state discovered by the other two pillars and turns it into evidence that counts everywhere it genuinely applies.



Gather the evidence once. It counts everywhere it applies.

Your access control policy is the same policy whether the auditor is asking under ISO 27001, Cyber Essentials or NCA ECC. 1,936 control-level cross-mappings mean you attach it once and it satisfies every requirement mapped to it, across all 31 frameworks in the catalogue.

31

frameworks plus a MITRE
ATT&CK threat layer

1,999

controls catalogued, 1,381
sub-controls

1,936

cross-mappings — 181
audit-proof

WHAT IT DOES — AND WHAT CHANGES WHEN IT DOES

CAPABILITY	WHAT IT GIVES YOU	WHAT CHANGES
AI-guided compliance assessment	A guided path through a framework that asks for what it needs, in order, in plain English.	The assessment stops being a two-hundred-row spreadsheet that one person dreads and everyone else avoids.
Thirty-one frameworks in one catalogue	ISO 27001, Cyber Essentials, NIST CSF, PCI DSS, NIS2, DORA, UK GDPR, NCA ECC, SAMA CSF, ADHICS and more — already mapped.	When a customer asks for a framework you have never run, it is already in the catalogue rather than a procurement decision.
Control-level cross-mapping	1,936 mappings between controls across frameworks, 181 of them drawn from a published crosswalk.	Overlapping requirements stop being reconciled by hand in a spreadsheet nobody trusts.
Evidence Vault with reuse tracking	Evidence attached to a control once, then counted against every framework requirement mapped to that control — with the reuse visible.	The second framework costs a fraction of the first. The third costs less again.
Evidenced, Declared or Unknown status	Every capability marked by how well it is actually proven, rather than a binary tick.	You know which of your controls would survive a challenge and which are currently taken on trust.
Policy generation and Policy Vault	Policies drafted for your organisation specifically, with branded PDF export and a single place they live.	You stop paying a consultant to re-badge a template you could not then keep current.
Controls Vault with AI-assisted validation	A structured control library with assisted review of what you have written against what the framework asked for.	A weak control description gets caught before an auditor catches it.
Security Universe on every plan	The complete cross-framework map, viewable on every tier including the entry plan, regardless of how many frameworks are active.	You can see what a future framework would demand before committing to it — and you are never charged per framework.
Third-party report ingestion	External pen test reports and existing scanner output uploaded into the Evidence Vault as evidence in their own right, against the controls they support.	The tools and providers you already pay for start earning their keep.

Where it fits, and what to read next

For everyday security

A guided assessment tells you where your gaps actually are, in plain English and in priority order — worth doing whether or not you ever show it to an auditor.

For compliance

The same assessment produces the evidence and control coverage a framework requires, reused automatically wherever it applies, instead of being gathered again for every new requirement.

The home of continuous controls monitoring

Compliance status evidenced on an ongoing basis rather than self-attested once a year in a spreadsheet. MFA state syncs live from your identity provider in Environment & People; remediation work in Technology & Threats arrives already attached to the control it evidences. The two other pillars are what make this one continuous rather than periodic.

THREE MOTIONS IN THIS PILLAR — CONTINUOUS, NEVER A STEP

IDENTIFY & AGGREGATE

Every framework you answer to, and the evidence you already hold — policies, reports, scan output, directory data — gathered once into the Evidence Vault.

PROTECT & VALIDATE

Each control marked Evidenced, Declared or Unknown. Policies drafted for your organisation and validated against the frameworks they serve. A green tick never means "someone said so".

UNIFY & MANAGE

One control model across 31 frameworks — evidence gathered for one counts everywhere it genuinely applies, and stays current between audits, not just on the day.

THE POINT PRODUCTS THIS COVERS

- GRC / compliance automation — Compliance Engine & Security Universe
- Policy & evidence tooling — Policy Vault & Evidence Vault
- Controls libraries and audit-readiness tooling
- Evidence-collection tooling

WHAT IT CONNECTS TO

- 31 compliance frameworks plus MITRE ATT&CK and the Unified Kill Chain
- Live evidence from Environment & People and Technology & Threats
- Third-party pen test reports and existing scanner output
- A published CIS to CJIS crosswalk for audit-proof mappings

Run one framework free and see the mapping work

Start an assessment on the free trial and watch a single piece of evidence satisfy requirements in frameworks you have not even activated yet. That is the whole argument for doing compliance in one place, and it takes about twenty minutes to prove.

[Start free for 14 days — no card](#)
[Book a walkthrough](#)
786cyber.com

FURTHER READING

Environment & People data sheet

Know what you have — the people and asset evidence this pillar reads from.

Technology & Threats data sheet

Know your exposure — where remediation evidence comes from.

Framework one-pagers

Cyber Essentials, ISO 27001, NCA ECC and SAMA CSF — the specific path for each.

786 Cyber Platform Overview

The four-page introduction: three pillars, twelve point products, one platform.