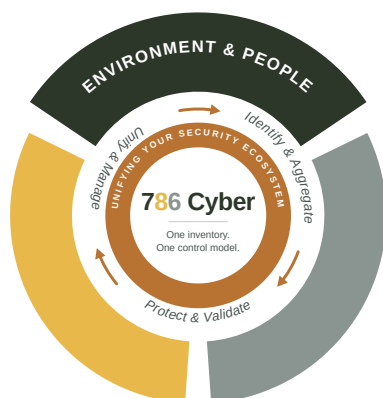


Know who and what can reach your data — and how.

Everything you run and everyone who can reach it, aggregated into a single inventory — the foundation the other two pillars read from.

You cannot protect what you have not found, and you cannot prove a control over people you cannot list. This pillar builds the inventory: it pulls your directory, your devices, your cloud, your domains and your external footprint into one place, links every asset to the person responsible for it, and keeps it current without anyone maintaining a spreadsheet.



This is where the single version of the truth gets built.

Every finding in Technology & Threats and every control in Policy & Process resolves back to an asset and a person that live here. Get this pillar right and the other two stop being guesswork.

7

asset types tracked in one directory

2

directory sources synced live

3

MFA states — never collapsed to a false "off"

WHAT IT DOES — AND WHAT CHANGES WHEN IT DOES

CAPABILITY	WHAT IT GIVES YOU	WHAT CHANGES
Directory sync — Microsoft 365 and Google Workspace	Every person, department, manager and usage location, updated automatically from the systems you already run.	Your people list stops being a spreadsheet that someone forgot to update in March.
Multi-factor authentication coverage	Exactly who has MFA enabled, disabled, or in an unknown state — tracked as three distinct values, not two.	You stop guessing at the single control auditors and insurers ask about most, and you can see the gap shrinking week by week.
Credential-breach and dark-web exposure	Which of your people appear in known breach corpora, checked continuously against Have I Been Pwned and XON.	You find out a credential is circulating before someone else finds a use for it.
Asset Intelligence — seven asset types	Servers, endpoints, network devices, cloud resources, applications, domains and more — with owner, serial, manufacturer, model and operating system.	"We didn't know that server existed" stops being a sentence anyone in your organisation has to say.
Asset-to-person reconciliation	Every device tied to the person accountable for it, and every person to the devices they hold.	A leaver becomes a checklist you can complete in an afternoon rather than an archaeology project.
External domain and subdomain discovery	The estate the outside world can see, discovered from certificate transparency logs and DNS rather than from memory.	Shadow infrastructure — the forgotten staging site, the subdomain from a campaign three years ago — surfaces before it is exploited.
Network connections graph	How assets relate to one another, drawn rather than described.	Blast radius becomes something you can see instead of something you argue about after an incident.
Software inventory and SBOM export	A machine-readable CycloneDX inventory of what runs where.	You answer a supply-chain questionnaire with a file, not a fortnight.
Identity posture scoring	One tracked measure of identity risk, built from MFA coverage and credential exposure.	You can show a board a trend line instead of an anecdote.

Where it fits, and what to read next

For everyday security

See at a glance which staff lack multi-factor authentication, whose credentials have appeared in a breach, and what devices, domains and cloud assets you actually have — before an attacker builds that list for you.

For compliance

An accurate people directory and asset inventory underpin access-control, joiner-mover-leaver and asset-management requirements across every framework in the catalogue. This is evidence you already have rather than evidence you go and build.

How it feeds the other two pillars

MFA state syncs live from your identity provider and feeds continuous controls monitoring in Policy & Process. The asset and network inventory feeds continuous posture management in Technology & Threats, so a vulnerability arrives already knowing which machine it sits on and who owns that machine. One inventory, one control model — not a separate spreadsheet per discipline.

THREE MOTIONS IN THIS PILLAR — CONTINUOUS, NEVER A STEP

IDENTIFY & AGGREGATE

Every account, device, cloud service, domain and subdomain from every connected source — Microsoft 365, Google Workspace, AWS, CSV, manual entry — into one inventory, with an owner against each.

PROTECT & VALIDATE

MFA read live in three states — enabled, disabled, unknown — dormant accounts flagged, credentials checked against breach data. Declared state is never taken on trust.

UNIFY & MANAGE

One directory and one asset register that the other two pillars and every framework read from, with joiners, movers and leavers tracked as they happen.

THE POINT PRODUCTS THIS COVERS

- Identity governance (IGA) — People Directory & Identity Posture
- Dark-web monitoring — Credential Breach Monitoring
- Asset inventory (CAASM) — Asset Intelligence
- SBOM tooling — Software Inventory & SBOM

WHAT IT CONNECTS TO

- Microsoft 365 and Microsoft Entra ID
- Google Workspace directory and devices
- Have I Been Pwned and XON breach intelligence
- Certificate transparency logs and DNS for external discovery
- CSV import, API and manual entry for everything else

See your own environment inside an hour

Connect one directory and one domain on the free trial. You will have a live inventory of your people, your assets and your external footprint the same day — including, in our experience, several things nobody expected to find.

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

FURTHER READING

Technology & Threats data sheet

Know your exposure — what threatens the estate mapped here, ranked by what attackers are exploiting.

Policy & Process data sheet

Prove it — how this inventory becomes evidence against 31 frameworks.

786 Cyber Platform Overview

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

Comparison — 786 Cyber vs. point solutions

What buying CAASM and IGA separately would cost, and why you keep what you have.