



Three pillars. Twelve point products. One platform.

Continuous compliance. Continuous posture management. Continuous threat exposure management — everything a complete security programme needs, built in, sharing one inventory and one control model. And whatever you already run comes in as evidence alongside it.

THREE MOTIONS — CONTINUOUS, ACROSS EVERY PILLAR

They run at the same time, across all three pillars. None of them is a step.

IDENTIFY & AGGREGATE

Everything you run, in one inventory

Your directory, your devices, your cloud accounts, your domains, your existing scanner output, your last pen test report. It arrives by sync, by import, by API or typed in by hand — and it all lands in **one inventory** instead of six systems that don't know about each other.

PROTECT & VALIDATE

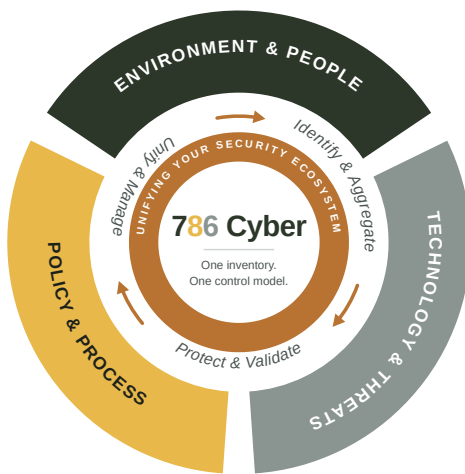
What it actually covers, not what you were told

Having a tool is not the same as being covered by it. We read the live state — is multi-factor authentication actually on, is that agent actually reporting, does that control actually have evidence behind it — and mark every capability **Evidenced, Declared or Unknown**.

UNIFY & MANAGE

One picture, managed continuously

Everything resolves into a single result — **one inventory, one control model, one answer** — and it stays current. New device, new starter, new vulnerability, new exposure: your position updates and you are told what changed and what to do about it.



Already have a scanner? Good.

It means you take hygiene seriously. Bring the report and the asset data in and they become evidence against the controls they support. Then we go further: every finding is validated against our own feeds, we keep aggregating your assets from every connected directory and cloud account so nothing the scan missed stays missed, and we prioritise by what your scanner can't see — asset importance, the controls already in place, and what your frameworks require. Ours runs alongside, at no extra charge.

THE TWELVE POINT PRODUCTS — AND WHICH PILLAR EACH ONE BELONGS TO

People Directory & Identity Posture IDENTITY GOVERNANCE (IGA)	Credential Breach Monitoring DARK-WEB MONITORING	Asset Intelligence ASSET INVENTORY (CAASM)	Software Inventory & SBOM SBOM TOOLING	Vulnerability Prioritisation VULNERABILITY MANAGEMENT (VM)	Cloud Posture CLOUD POSTURE (CSPM)
Web Application Scanning WEB APP SCANNING (DAST)	External Attack Surface EXTERNAL ATTACK SURFACE (EASM)	Threat Intelligence & Reputation THREAT INTELLIGENCE (CTI)	Testing & Validation PEN-TEST TOOLING	Compliance Engine & Security Universe GRC / COMPLIANCE AUTOMATION	Policy Vault & Evidence Vault POLICY & EVIDENCE TOOLING

■ Environment & People
 ■ Technology & Threats
 ■ Policy & Process

Twelve things you would otherwise buy separately — sharing one inventory and one control model. Detail on page 3.

Your organisation, read from your systems.

Connect Microsoft 365, Google Workspace, your cloud accounts and your domains — or import a spreadsheet, or add records by hand. However it arrives, it lands in **one inventory** that everything else reads from. Illustrative views below.

248
PEOPLE

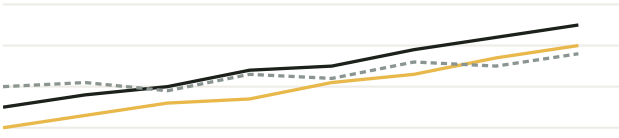
412
ASSETS ACROSS 7
TYPES

17
WITHOUT MFA

6
CREDENTIALS IN A
BREACH

Posture trend

Independent lanes, 90 days — never one blended number



— Identity — Compliance - - Vulnerability. Each lane scored on its own terms.

Findings by exploitability

Ranked by EPSS and CISA KEV, not raw severity

Known exploited (KEV) 4

EPSS > 10% 11

EPSS 1–10% 38

EPSS < 1% 204

257 findings. Four of them are being exploited in the wild today. Those four are the queue.

MFA coverage

Three states, never two

85%

■ Enabled 211
■ Disabled 17
■ Unknown 20

"Unknown" is never collapsed into "off". You are told what we cannot see.

Network connections

Assets, owners and what talks to what



Copper marks an asset with a live finding. Follow the edge to its owner.

People and departments

Synced, or imported, or entered by hand



Staff, contractors and service accounts — from M365, Google, CSV or manual entry.

Compliance, evidenced

Evidenced / Declared / Unknown — never a green tick that means "someone said so"

Cyber Essentials Plus 81%

ISO/IEC 27001 57%

UK GDPR 69%

Evidence gathered for one framework counts everywhere it genuinely applies — 1,936 cross-mappings decide where.

The queue

What to fix first, and why

FINDING	ASSET	WHY NOW
CVE-2026-3184	web-prod-02	KEV
Public S3 bucket	aws-eu-w2	EXPOSED
CVE-2026-1177	fin-lap-114	EPSS 31%
Expired TLS cert	portal.—.com	30 DAYS
Admin, no MFA	3 accounts	IDENTITY

Every row carries a plain-English explanation and the control it evidences.

786 Cyber · 786cyber.com · Illustrative views. Your figures will differ.

Platform overview · v14.0 · page 2 of 4



Three pillars. Everything maps to one of them.

The pillars are not product categories — they are the three dimensions of a complete security programme, and they run at the same time. Some of these you may already run elsewhere and we aggregate; some we validate; the rest we provide natively. **All of it unifies into one result.**

Environment & People

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

People Directory & Identity Posture

Every person, their access and their MFA state — read live from Microsoft 365 or Google Workspace, never re-declared.

IDENTITY GOVERNANCE (IGA)

Credential Breach Monitoring

Breached credentials tied to your domains, surfaced before they are used against you.

DARK-WEB MONITORING

Asset Intelligence

Every device, cloud service, domain and subdomain in one inventory — with an owner, and what it talks to.

ASSET INVENTORY (CAASM)

Software Inventory & SBOM

Installed software on every asset, matched to CVEs, exported as CycloneDX.

SBOM TOOLING

Technology & Threats

Know your exposure. Manage the risks that matter to your business.

Vulnerability Prioritisation

Findings scored by EPSS exploit probability and CISA KEV, not raw CVSS — each explained in plain English.

VULNERABILITY MANAGEMENT (VM)

Cloud Posture

AWS, Azure and GCP checked against CIS Benchmarks through a read-only, revocable role.

CLOUD POSTURE (CSPM)

Web Application Scanning

OWASP ZAP baseline scans on every domain you register, findings mapped to the controls they affect.

WEB APP SCANNING (DAST)

External Attack Surface

Exposed services, weak TLS, certificate changes and look-alike domains — the outside-in view.

EXTERNAL ATTACK SURFACE (EASM)

Threat Intelligence & Reputation

Open-source intelligence and reputation feeds, prioritised against your assets rather than the internet at large.

THREAT INTELLIGENCE (CTI)

Testing & Validation

Consented, admin-gated active testing against your own estate — deliberately kept out of your posture score.

PEN-TEST TOOLING

Policy & Process

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

Compliance Engine & Security Universe

31 frameworks, 1,999 controls, one control model — evidence gathered once counts everywhere it genuinely applies.

GRC / COMPLIANCE AUTOMATION

Policy Vault & Evidence Vault

Policies drafted for your organisation, controls validated, every capability marked Evidenced, Declared or Unknown.

POLICY & EVIDENCE TOOLING

However your data wants to arrive — including from tools that aren't ours

Directory sync from Microsoft 365 or Google Workspace. Read-only roles for AWS, Azure and GCP. Domain and subdomain discovery from certificate transparency and DNS. CSV import for anything else. Manual entry for contractors, service accounts and the things no system knows about. Third-party reports — an external pen test, an existing scanner's output — upload into the Evidence Vault as evidence in their own right. **Every route lands in the same inventory**, which is why a finding can know its asset, its owner and its control without anyone joining them up by hand.

Testing & Validation — deliberate, consented, and kept out of your score

Real active reconnaissance against your own estate: web application scanning and DNS, IP and application-layer tooling, gated to administrators and run only with explicit per-session consent. Results are shown clearly and **never feed the automatic posture score** — a test you chose to run at a moment you chose is not the same evidence as continuous monitoring, and blending the two would make the score look better and mean less. It sits inside Technology & Threats, alongside the continuous capabilities rather than mixed into them.



The first fourteen days, and a way in that costs nothing.

DAY 1

Connect

Microsoft 365 or Google Workspace, a domain and a cloud account — a read-only connection each, minutes not a project. By the end of the day you have every account with its MFA state, and the assets and subdomains you didn't know you had.

OAuth directory sync · AWS cross-account role · certificate transparency and DNS enumeration · CSV import

DAY 2

See

Exposed services, look-alike domains, credentials already in a breach, and your first prioritised queue — ranked by what attackers are exploiting, not by raw severity, each finding explained in plain English.

MFA tri-state · HIBP and XON · Shodan and Censys · CPE against NVD · EPSS and KEV · ZAP · Prowler

DAY 7

Prove

A gap report against your first framework, every control marked Evidenced, Declared or Unknown — and the evidence you already hold counted where it genuinely applies.

Canonical control model · 1,936 cross-mappings · Evidence Vault · Evidenced / Declared / Unknown

DAY 14

Stay

A new starter, a new device, a new vulnerability, a new exposure — you're told what changed and what to do. Pick a plan when you're ready; the mapping work you've done comes with you.

Continuous controls monitoring · continuous posture management · CTEM

PUBLISHED PRICING

Essentials

£249/mo

or £199/mo billed annually
compliance, plus automation
3 frameworks · scanning included

MOST POPULAR

Growth

£549/mo

or £439/mo billed annually
for a scaling security function
5 frameworks · 25 policies

Business

£1,199/mo

or £959/mo billed annually
for an established programme
10 frameworks · full policy library

Every plan maps the whole catalogue — all 31 frameworks are always visible and mappable in the Security Universe, at no extra cost; plans gate how many you actively run, never which ones. Just need to get compliant? **Comply** is £149/month for 2 frameworks with manual evidence — no automated scanning. **Enterprise** starts at £2,500/month for 20+ frameworks, dedicated data residency and an API. All prices ex-VAT; GBP, USD and SAR. Annual billing saves 20%.

START · PROVE · COMMIT

STAGE 1

Start

14 days free, no card. Connect your environment and see what's actually there.

Removes **risk** — nothing charged, nothing to cancel.

STAGE 2

Prove

Explore further on a single-month contract — cancel anytime, no long-term commitment.

Removes **commitment** — one month at a time, for as long as you want.

STAGE 3

Commit

Go annual for ongoing compliance, risk and threat management — and save 20%.

Removes **cost — and the procurement cycle**.

See what's actually there.

Connect your directory, a domain and a cloud account. Fourteen days, no card, no sales call — and you will find something you didn't know you had. 786cyber.com

GO DEEPER — THE DETAILED DATA SHEETS

Each pillar has a two-page data sheet that enlarges its segment of the Wheel and goes capability by capability through what it does, what it gives you, and what changes.

Environment & People

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

Technology & Threats

Know your exposure. Manage the risks that matter to your business.

Policy & Process

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

Also on 786cyber.com/downloads: the Testing & Validation sheet, the Cyber Essentials, ISO 27001, NCA ECC and SAMA CSF one-pagers, and the Partner & MSP data sheet.