

Where we cannot see — and what it is worth to fix

Demo — Sightline · Electric Utilities

ASSESSMENT	PREPARED BY	DATA REGION	REFERENCE
9 October 2026	Sightline (Agnostec)	UK (sovereign)	A-00050

We carry an estimated **£62k** a year in expected cyber loss (range £12k–£222k). Our measured visibility stands at **25/100** (+5 pts over 7 assessments), with **12** blind asset surfaces and **14** shadow surfaces; 5 of 6 crown jewels sit at the end of a measured attack route.

EXPECTED ANNUAL LOSS £62k range £12k–£222k	VISIBILITY 25/100 73 measured · 12 blind · 14 shadow	ATTACK ROUTES 12 8 choke points	CROWN JEWELS IN REACH 5/6 via measured blind/shadow routes
--	--	---	--

Confidential board material. Every figure is derived from Demo — Sightline's own evidence, processed in the UK. Monetary values are modelled ranges (sources in the appendix), never point certainties. The price to secure (section 6) is a market average for the technology category, not a quote — Demo — Sightline's own quotes replace it.

01 · EXECUTIVE SUMMARY

The position, and the decision

EXPECTED ANNUAL LOSS

£62k

range £12k–£222k

VISIBILITY SCORE

25/100

+5 pts since 2026-04

BLIND SPOTS

12

21 → 12 over 7 runs

ATTACK ROUTES

128 choke points · 5/6 crown
jewels in reach

What the board needs to know

- **Exposure.** revenue-at-risk: £180m × 0.034% (mean; median 0.015%) — the organisation-level anchor, allocated across 82 measured gaps by risk weight (loss-rate: Agnostec starter loss-rate (real-loss derived) 2026-draft-v1, utilities / medium).
- **Biggest risks.** Archives (Blind, £2.6k/yr); External Sharing Links (Shadow, £2.3k/yr); Data Access (Shadow, £2.2k/yr).
- **Visibility.** 73 asset surfaces are measured; 12 are blind (owned, unobserved) and 14 are shadow (observed, unowned). 85 of 155 in-scope behaviours are monitored.
- **Direction.** Exposure down 6.5% since last assessment — risk is being bought down. Visibility +5 pts; blind spots 21 → 12.
- **Crown jewels.** Utilities Operations, Industrial Control, Critical Safety Control, Customer Data, Revenue are reachable along measured blind/shadow routes.

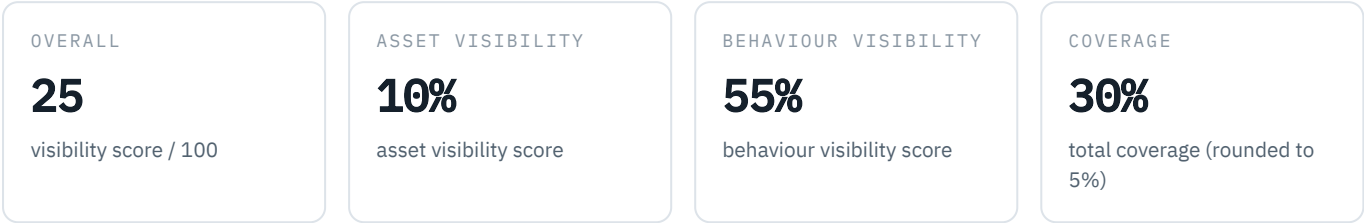
Recommended asks of the board

1. Mandate the **5 “Fix now”** remediation programmes (section 7, covering 31 surfaces): together they remove **£26k** (42.9%) of the £62k expected annual loss (Close residual gaps — identity & trust anchors; Close residual gaps — machine & execution surfaces; Close residual gaps — data & content surfaces and 2 more). Leaving them open costs that amount, every year.
2. Schedule the **6 “Next”** programmes behind them, a further **£13k** (21.5%) a year.
3. Within them, close the highest-loss surfaces first: Archives (£2.2k/yr), External Sharing Links (£2.0k/yr), Data Access (£1.9k/yr).
4. Prioritise the choke points **API Keys, Sensors, Databases** — each sits on several attack routes, so one fix breaks many.
5. Note the in-scope regulatory posture (section 4): NIS2, ISO/IEC 27001, NCSC CAF, Cyber Essentials.

02 · RISK POSTURE

How much of the estate we can see

Visibility is measured from Demo — Sightline's own inventories and telemetry. A surface counts only if the evidence shows it.

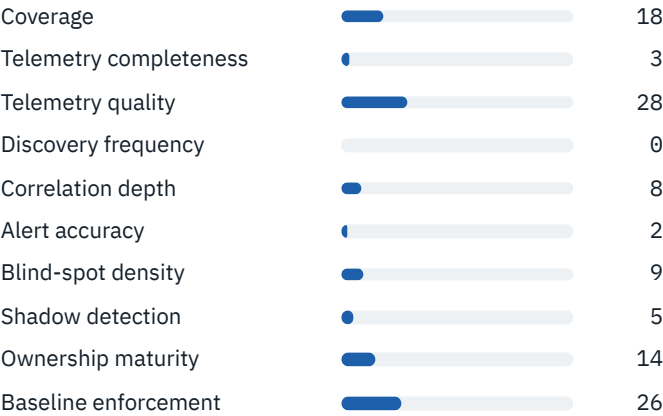


Evidence by layer



Surfaces evidenced per layer (assets + behaviours); bars show each layer's share of the surfaces evidenced.

Capability profile



Engine capability metrics, 0–100.

Measured · Blind · Shadow

STATE	SURFACES	MEANING
MEASURED	73	Owned and observed
BLIND	12	Owned, not observed
SHADOW	14	Observed, not owned

03 · PRIORITISED FINDINGS

Fix-first risks, in £

In remediation order — the expected annual loss each fix removes. That loss is the surface's share of the organisation's expected annual loss, by how much the business relies on it (its footprint and dependencies, with the Utilities & Energy baseline, enriched by your crown jewels) × how exposed the gap is × event frequency; closing the gap removes most, not all, of it. TCOI is the cost of leaving the surface as it is, every year. The order does not depend on the loss-rate assumption.

#	SURFACE & RECOMMENDED ACTION	STATE	PRIORITY	TCOI / YR	RANGE	LOSS AVOIDED / YR
01	Archives MODERATE L4 · Data & Content Surfaces · fully unmonitored → Instrument this surface. Apply data classification and DLP; confirm encryption at rest and access logging.	BLIND	39	£2.6k	£508–£9.5k	£2.2k
02	External Sharing Links MODERATE L4 · Data & Content Surfaces · unmanaged / off-baseline → Bring under inventory & baseline. Apply data classification and DLP; confirm encryption at rest and access logging.	SHADOW	34	£2.3k	£447–£8.3k	£2.0k
03	Data Access MODERATE L4 · Data & Content Surfaces · unmanaged / off-baseline → Bring under inventory & baseline. Apply data classification and DLP; confirm encryption at rest and access logging.	SHADOW	33	£2.2k	£430–£8.0k	£1.9k
04	API Keys BUSINESS-CRITICAL L2 · Identity & Trust Anchors · fully unmonitored → Instrument this surface. Enforce MFA, review privileged and service accounts, and monitor authentication events.	BLIND	72	£2.0k	£380–£7.1k	£1.7k
05	OAuth Apps SIGNIFICANT L2 · Identity & Trust Anchors · unmanaged / off-baseline → Bring under inventory & baseline. Enforce MFA, review privileged and service accounts, and monitor authentication events.	SHADOW	61	£1.7k	£325–£6.1k	£1.4k
06	Sensors BUSINESS-CRITICAL L8 · OT / ICS / Physical Surfaces · existential for Utilities & Energy; fully unmonitored → Instrument this surface. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning.	BLIND	100	£1.4k	£278–£5.2k	£1.2k
07	Printers SIGNIFICANT L3 · Machine & Execution Surfaces · fully unmonitored → Instrument this surface. Ensure EDR coverage and an enforced configuration baseline on these hosts.	BLIND	59	£1.4k	£276–£5.1k	£1.2k
08	Badge Readers BUSINESS-CRITICAL L8 · OT / ICS / Physical Surfaces · existential for Utilities & Energy; fully unmonitored → Instrument this surface. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning.	BLIND	94	£1.4k	£260–£4.9k	£1.1k

#	SURFACE & RECOMMENDED ACTION	STATE	PRIORITY	TCOI / YR	RANGE	LOSS AVOIDED / YR
09	Environmental Sensors BUSINESS-CRITICAL L8 · OT / ICS / Physical Surfaces · existential for Utilities & Energy; fully unmonitored → Instrument this surface. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning.	BLIND	90	£1.3k	£249–£4.7k	£1.1k
10	Building Management Systems (BMS) BUSINESS-CRITICAL L8 · OT / ICS / Physical Surfaces · existential for Utilities & Energy; fully unmonitored → Instrument this surface. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning.	BLIND	90	£1.3k	£248–£4.6k	£1.1k
11	Edge Compute Nodes SIGNIFICANT L3 · Machine & Execution Surfaces · fully unmonitored → Instrument this surface. Ensure EDR coverage and an enforced configuration baseline on these hosts.	BLIND	52	£1.3k	£245–£4.6k	£1.1k
12	Unintegrated M&A Infrastructure SIGNIFICANT L3 · Machine & Execution Surfaces · unmanaged / off-baseline → Bring under inventory & baseline. Ensure EDR coverage and an enforced configuration baseline on these hosts.	SHADOW	53	£1.3k	£245–£4.6k	£1.1k
13	Unmanaged Devices SIGNIFICANT L3 · Machine & Execution Surfaces · unmanaged / off-baseline → Bring under inventory & baseline. Ensure EDR coverage and an enforced configuration baseline on these hosts.	SHADOW	51	£1.2k	£236–£4.4k	£1.0k
14	OT Remote Access Surfaces BUSINESS-CRITICAL L8 · OT / ICS / Physical Surfaces · existential for Utilities & Energy; unmanaged / off-baseline → Bring under inventory & baseline. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning.	SHADOW	84	£1.2k	£233–£4.3k	£1.0k
15	AI Agents SIGNIFICANT L3 · Machine & Execution Surfaces · 12 monitored behaviours depend on it; 75% unobserved → Close the residual gaps. Ensure EDR coverage and an enforced configuration baseline on these hosts.	MEASURED	53	£1.3k	£245–£4.6k	£1.0k
16	SaaS Identities SIGNIFICANT L2 · Identity & Trust Anchors · 2385 assets — central to the estate; 50% unobserved → Close the residual gaps. Enforce MFA, review privileged and service accounts, and monitor authentication events.	MEASURED	52	£1.4k	£274–£5.1k	£995

Top 16 of 82 measured gaps shown; together they carry £25k of the £62k expected annual loss. Hover-level sources for every figure are in the appendix.

04 · VISIBILITY GAPS & REGULATORY POSTURE

What we own but cannot see — and what we see but do not own

Blind surfaces 12

SURFACE	LAYER	INV.	TEL.	BLIND
Sensors	L8 OT	640	0	640
Environmental Sensors	L8 OT	304	0	304
Badge Readers	L8 OT	212	0	212
API Keys	L2 Identity	121	0	121
Printers	L3 Machine	87	0	87
Suppliers	L1 Human	64	0	64
SD-WAN Infrastructure	L5 Network	46	0	46
Edge Compute Nodes	L3 Machine	31	0	31
Databases	L6 Application	20	0	20
Archives	L4 Data	12	0	12
MSP Remote Access Pathways	L7 Supply	9	0	9
Building Management Systems (BMS)	L8 OT	9	0	9

Shadow surfaces 14

SURFACE	LAYER	INV.	TEL.	SHADOW
Logging & Monitoring	L9 Detection	0	45	45
OAuth Apps	L2 Identity	0	41	41
External Sharing Links	L4 Data	0	41	41
Unintegrated M&A Infrastructure	L3 Machine	0	41	41
Cloud Logs	L9 Detection	0	33	33
Unmanaged Devices	L3 Machine	0	32	32
Data Access	L4 Data	0	25	25
Shadow SaaS	L6 Application	0	23	23
Cloud Networking	L5 Network	0	20	20
Exposed Services	L5 Network	0	18	18
Cloud Security	L9 Detection	0	15	15
Orphaned/Stale Human Accounts	L1 Human	0	12	12
CASB	L9 Detection	0	10	10
OT Remote Access Surfaces	L8 OT	0	5	5

Framework posture

FRAMEWORK (IN SCOPE)	OBJECTIVES TOUCHED	EXPOSURE	OBJECTIVES UNDER MOST PRESSURE
NIS2 EU directive · Operator of an essential service	13	£107k	Security in acquisition/dev 21(2)(e) £18k Access control & asset mgmt 21(2)(i) £14k MFA & secured comms 21(2)(j) £14k
ISO/IEC 27001 International · Voluntary but commonly required by customers/insurers	11	£86k	A.8 Technological (access control) £14k A.5 Organizational £14k A.8 Technological (cryptography & data) £14k

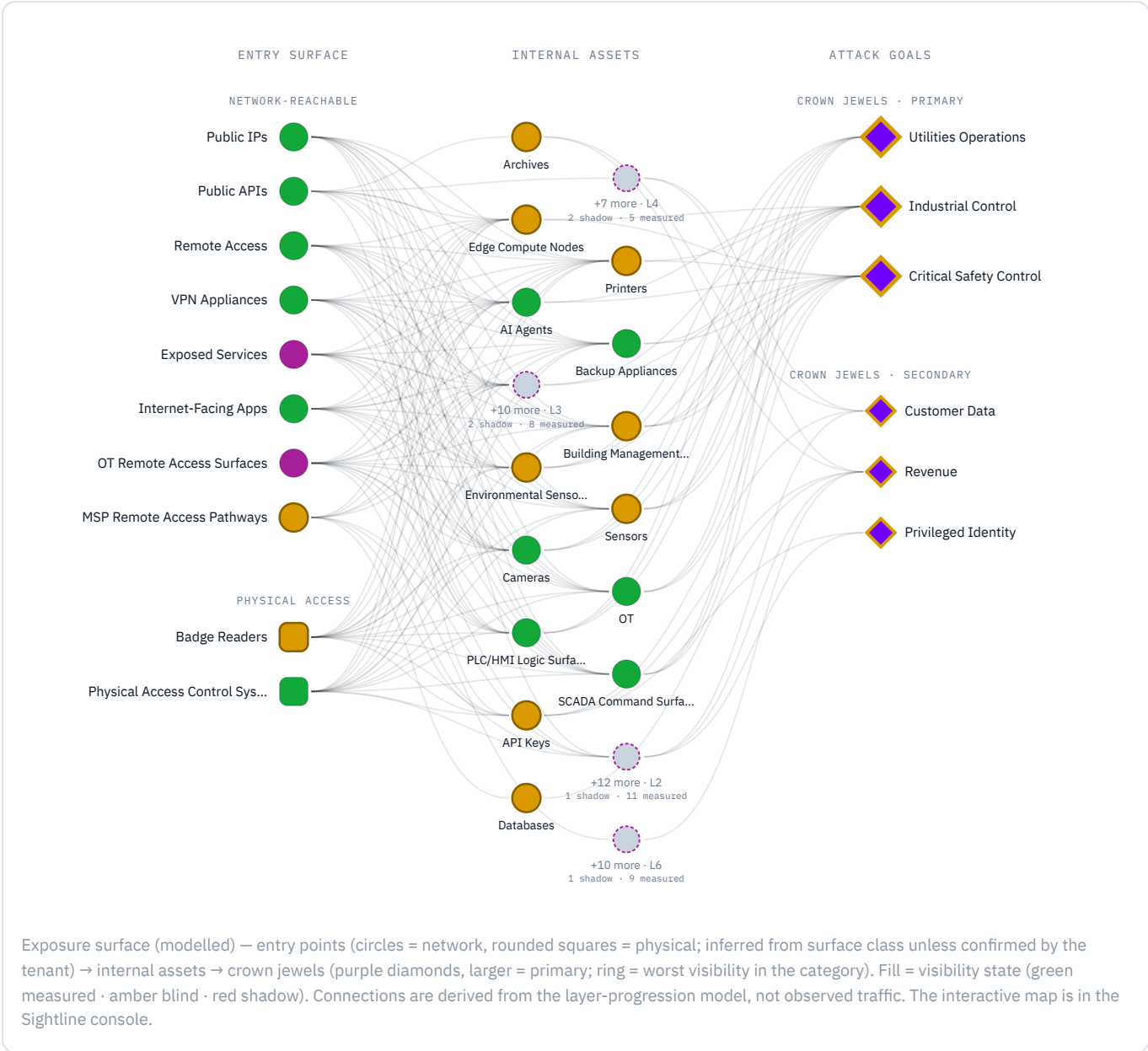
FRAMEWORK (IN SCOPE)	OBJECTIVES TOUCHED	EXPOSURE	OBJECTIVES UNDER MOST PRESSURE
NCSC CAF UK (CNI/NIS) · UK operator of essential services	10	£79k	B4 System security £18k B2 Identity & access control £14k B3 Data security £14k
Cyber Essentials UK scheme · UK baseline; often a contractual / public-sector floor	5	£78k	Secure configuration £32k Security update management £16k User access control £14k

Indicative control-objective mapping — not a compliance assessment or legal attestation. Validate against current framework text.

05 · ATTACK ROUTES

How blindness chains toward the crown jewels

Routes across measured blind and shadow surfaces, following a documented standard-attack progression between layers. Each hop is a gap Sightline measured — this shows where an attacker could move undetected, not a prediction or an exploit chain.



Exposure surface (modelled) — entry points (circles = network, rounded squares = physical; inferred from surface class unless confirmed by the tenant) → internal assets → crown jewels (purple diamonds, larger = primary; ring = worst visibility in the category). Fill = visibility state (green measured · amber blind · red shadow). Connections are derived from the layer-progression model, not observed traffic. The interactive map is in the Sightline console.

Choke points: API Keys (on 8 routes) · Sensors (on 8 routes) · Databases (on 7 routes) · Suppliers (on 6 routes) · Printers (on 4 routes) · Archives (on 4 routes) — fixing one breaks several routes at once.

#	ROUTE	HOPS	WEAKEST LINK	£ AT TARGET
01	Suppliers → Databases → API Keys → Sensors	4	Suppliers	£1.4k
02	Databases → Printers → SD-WAN Infrastructure → Sensors	4	Databases	£1.4k

#	ROUTE	HOPS	WEAKEST LINK	£ AT TARGET
03	MSP Remote Access Pathways → Printers → SD-WAN Infrastructure → Sensors	4	MSP Remote Access Pathways	£1.4k
04	MSP Remote Access Pathways → Databases → API Keys → Sensors	4	MSP Remote Access Pathways	£1.4k
05	Suppliers → API Keys → Sensors	3	Suppliers	£1.4k
06	Databases → API Keys → Sensors	3	Databases	£1.4k
07	MSP Remote Access Pathways → API Keys → Sensors	3	MSP Remote Access Pathways	£1.4k
08	SD-WAN Infrastructure → Sensors	2	SD-WAN Infrastructure	£1.4k

06 · BOARD CASE

What it costs to secure — and what that's worth

AT PRESENT

25/100

visibility score · 76 gapped surfaces across 8 programmes

COST OF DOING NOTHING

£59k/yr expected · £1.63m if breached

REMEDiate →

31

distinct controls, each bought once

INVESTMENT

£559k/yr

SECURE

~86%

of addressed loss removed (effectiveness, weighted by ALE)

RESIDUAL LOSS

£8.5k/yr expected · £235k if breached

LOSS REMOVED

£50k/yr · £1.40m if breached

£0 · green £1.40m removed · amber £235k residual

£1.63m if breached

£559k/yr secures ~86% of your £1.63m single-incident exposure.

EXPECTED ANNUAL LOSS

£59k

across 8 programmes · 76 gaps

LOSS IF BREACHED

£1.63m

single incident: expected annual ÷ 3.6% incidence

TO SECURE / YR

£559k

31 controls bought once (rows £747k)

NET BENEFIT / YR

–£508k

£50k removed – buy-once price · £8.5k remains

If breached: £1.63m exposure → £235k after securing · £1.40m removed for £559k a year. The single-incident view, alongside the expected year — net benefit above stays measured against expected loss.

PROGRAMME & SECURED BY	ALE	LOSS IF BREACHED	GAPS	PRICE TO SECURE	EFFECTIVE-NESS	ALE AFTER	NET BENEFIT (EXPECTED)	NET BENEFIT (IF BREACHED)	SEVERITY	VALUE
L5 · Network & Connectivity SASE / SSE (converged) · CSPM / CNAPP · External Attack Surface Mgmt (EASM) · Next-Gen Firewall (NGFW) — subscription · Web Application Firewall (WAF) · Network Access Control (NAC) · Zero Trust Network Access / VPN (ZTNA) · DNS Security / Protective DNS	£1.5k	£43k	11	£105k	90%	£153	–£103k	–£66k	48.9	8.1

Sightline by Agnostec · UK-hosted · UK data region

Page 10 of 18

PROGRAMME & SECURED BY	ALE	LOSS IF BREACHED	GAPS	PRICE TO SECURE	EFFECTIVE- NESS	ALE AFTER	NET BENEFIT (EXPECTED)	NET BENEFIT (IF BREACHED)	SEVERITY	VALUE
L8 · OT / ICS / Physical IoT Security · Physical Access Control (PACS) — software · OT / ICS Security Monitoring · Zero Trust Network Access / VPN (ZTNA)	£9.8k	£274k	10	£92k	81%	£1.9k	-£84k	+£130k	48.4	7
L2 · Identity & Trust Anchors Secrets Management · SaaS Security Posture Mgmt (SSPM) · Multi- Factor Authentication (MFA) · Privileged Access Management (PAM) · PKI / Certificate Lifecycle Mgmt · Cloud Infra Entitlement Mgmt (CIEM)	£14k	£402k	12	£101k	90%	£1.4k	-£88k	+£260k	43	8.2
L7 · Supply Chain & Trust Chain Privileged Access Management (PAM) · Third- Party / Vendor Risk Mgmt (TPRM) · External Attack Surface Mgmt (EASM)	£360	£10k	5	£49k	82%	£65	-£49k	-£41k	37.8	5.8
L4 · Data & Content Backup & Disaster Recovery · Cloud Access Security Broker (CASB) · Data Security Posture Mgmt (DSPM)	£14k	£381k	8	£58k	80%	£2.7k	-£47k	+£246k	35.8	7.1

PROGRAMME & SECURED BY	ALE	LOSS IF BREACHED	GAPS	PRICE TO SECURE	EFFECTIVE- NESS	ALE AFTER	NET BENEFIT (EXPECTED)	NET BENEFIT (IF BREACHED)	SEVERITY	VALUE
L3 · Machine & Execution Network Access Control (NAC) · AI Security Posture / LLM Security · Cyber Asset Attack Surface Mgmt (CAASM) · CSPM / CNAPP · Endpoint Protection / EDR / XDR · Mobile Threat Defense (MTD) · Container & Kubernetes Security · Backup & Disaster Recovery	£13k	£364k	14	£160k	90%	£1.3k	-£148k	+£168k	35.6	4.7
L1 · Human Surfaces Third-Party / Vendor Risk Mgmt (TPRM) · Security Awareness Training · Identity Governance & Admin (IGA) · Privileged Access Management (PAM) · Multi- Factor Authentication (MFA)	£823	£23k	6	£66k	90%	£82	-£65k	-£45k	30.8	4.1
L6 · Application, SaaS & Browser Data Security Posture Mgmt (DSPM) · Cloud Access Security Broker (CASB) · AppSec Testing (SAST/DAST/SCA) · Software Supply Chain / SBOM · SaaS Security Posture Mgmt (SSPM) · API Security	£4.9k	£136k	10	£116k	84%	£808	-£112k	-£1.9k	28.2	4.1
L10 · AI & Autonomous Behaviour — No measured gap — not in the totals.	£0	£0	0	£0	0%	£0	+£0	+£0	0	0

PROGRAMME & SECURED BY	ALE	LOSS IF BREACHED	GAPS	PRICE TO SECURE	EFFECTIVE- NESS	ALE AFTER	NET BENEFIT (EXPECTED)	NET BENEFIT (IF BREACHED)	SEVERITY	VALUE
Total (8 programmes, buy-once price)	£59k	£1.63m	76	£559k		£8.5k	-£508k	+£838k		

Against a single incident, programmes above the line remove more loss than they cost; those below are insurance against a hit that would otherwise be far larger.

Ordered by severity (dependency × exposure). Gaps = surfaces with any blind or shadow instances; secured by = the distinct primary control of each gapped surface (never the layer's whole stack). Loss if breached = the modelled cost of a single incident — expected annual loss ÷ 3.6% annual incidence (Cyentia IRIS 2025 sector × size incidence (utilities / medium) — loss-rate-methodology.md §5a). Net benefit (expected) = (ALE — ALE after) — price; net benefit (if breached) = (loss if breached — loss after) — price; totals use the buy-once price (shared controls counted once). Value = dependency secured per £1k. Effectiveness = overlap-aware (strongest control full credit; each weaker one 35% of its effect on the risk still remaining), capped at 90% — the potential when properly deployed; no control-maturity discount is applied. Prices: market averages on Demo — Sightline's estate at the Medium (£100m–1bn) volume discount (not quotes; hardware capex and professional services excluded). Demo estate figures are illustrative — a medium regional utility (£180m turnover). Layer 9 is the control stack that secures the others and is not priced as its own row. All figures modelled.

07 · REMEDIATION PLAN

What to fix, in what order, and who owns it

FIX NOW — LOSS AVOIDED

£26k / yr

5 programmes · 31 surfaces · 42.9% of expected annual loss

EVERY GAP CLOSED — LOSS AVOIDED

£48k / yr

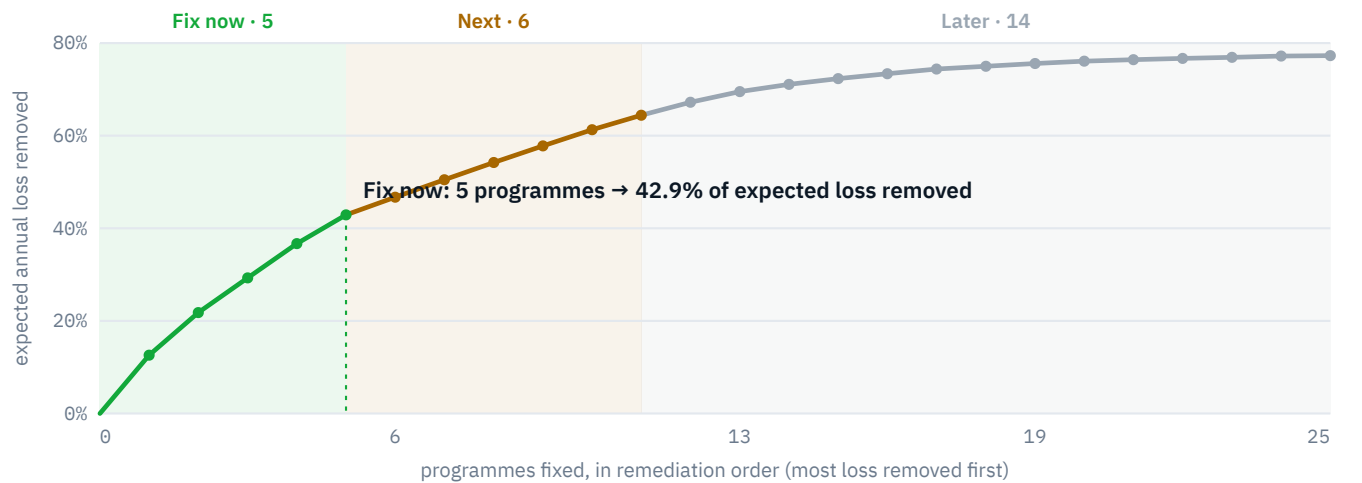
77.3% removed · £14k remains

SAVED SCENARIO

43%

31 fixes · £26k / yr · 6/6 routes broken

How fast the loss comes down



Remediation order — by expected loss removed

#	PROGRAMME & WHAT'S NEEDED	TIER	LOSS / YR	LOSS AVOIDED / YR	ROUTES	CUMULATIVE
01	Close residual gaps — identity & trust anchors Close the residual gaps. Enforce MFA, review privileged and service accounts, and monitor authentication events. Covers SaaS Identities, Authentication Events, SSH Keys, MFA Tokens +6 more.	FIX NOW	£11k	£7.8k	0/6	12.6%
02	Close residual gaps — machine & execution surfaces Close the residual gaps. Ensure EDR coverage and an enforced configuration baseline on these hosts. Covers AI Agents, Endpoints, Servers, Mobile Devices +6 more.	FIX NOW	£7.9k	£5.7k	0/6	21.8%
03	Close residual gaps — data & content surfaces Close the residual gaps. Apply data classification and DLP; confirm encryption at rest and access logging. Covers File Shares, Cloud Storage, Data Lakes, Warehouses +1 more.	FIX NOW	£6.5k	£4.6k	0/6	29.3%
04	Instrument — OT / ICS / physical Instrument. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning. Covers Sensors, Badge Readers, Environmental Sensors, Building Management Systems (BMS).	FIX NOW	£5.4k	£4.6k	6/6	36.7%
05	Inventory & baseline — data & content surfaces Bring under inventory & baseline. Apply data classification and DLP; confirm encryption at rest and access logging. Covers External Sharing Links, Data Access.	FIX NOW	£4.5k	£3.9k	0/6	42.9%

#	PROGRAMME & WHAT'S NEEDED	TIER	LOSS / YR	LOSS AVOIDED / YR	ROUTES	CUMULATIVE
Fix now ends here — 5 programmes, 42.9% of the expected annual loss removed.						
06	Close residual gaps — applications, SaaS & browser Close the residual gaps. Turn on application/WAF logging and review exposed endpoints and SaaS grants. Covers Internal Applications, Code Repos, SaaS Tenants, CI/CD Pipelines +4 more.	NEXT	£3.4k	£2.3k	0/6	46.7%
07	Close residual gaps — OT / ICS / physical Close the residual gaps. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning. Covers OT, Cameras, Physical Access Control Systems, PLC/HMI Logic Surfaces +1 more.	NEXT	£3.3k	£2.3k	0/6	50.5%
08	Instrument — machine & execution surfaces Instrument. Ensure EDR coverage and an enforced configuration baseline on these hosts. Covers Printers, Edge Compute Nodes.	NEXT	£2.7k	£2.3k	2/6	54.2%
09	Instrument — data & content surfaces Instrument. Apply data classification and DLP; confirm encryption at rest and access logging. Covers Archives.	NEXT	£2.6k	£2.2k	0/6	57.8%
10	Inventory & baseline — machine & execution surfaces Bring under inventory & baseline. Ensure EDR coverage and an enforced configuration baseline on these hosts. Covers Unintegrated M&A Infrastructure, Unmanaged Devices.	NEXT	£2.5k	£2.1k	0/6	61.3%
11	Inventory & baseline — detection & control gaps Bring under inventory & baseline. Validate detection coverage for this control and tune alerting to cut blind spots. Covers CASB, Cloud Logs, Logging & Monitoring, Cloud Security.	NEXT	£2.3k	£1.9k	0/6	64.4%
12	Instrument — identity & trust anchors Instrument. Enforce MFA, review privileged and service accounts, and monitor authentication events. Covers API Keys.	LATER	£2.0k	£1.7k	4/6	67.2%
13	Inventory & baseline — identity & trust anchors Bring under inventory & baseline. Enforce MFA, review privileged and service accounts, and monitor authentication events. Covers OAuth Apps.	LATER	£1.7k	£1.4k	0/6	69.5%
14	Inventory & baseline — OT / ICS / physical Bring under inventory & baseline. Segment OT from IT and deploy passive OT/ICS monitoring; no active scanning. Covers OT Remote Access Surfaces.	LATER	£1.2k	£1.0k	0/6	71.1%

Showing the first 14 of 25 programmes.

Ownership & status

FIX	OWNER	TARGET	STATUS	VERIFICATION
Sensors	Data Protection Officer	2026-10-16	IN PROGRESS	next assessment
Badge Readers	IT Infrastructure Lead	2026-11-16	DEFERRED	next assessment
Environmental Sensors	Identity & Access Lead	2026-11-09	IN PROGRESS	next assessment

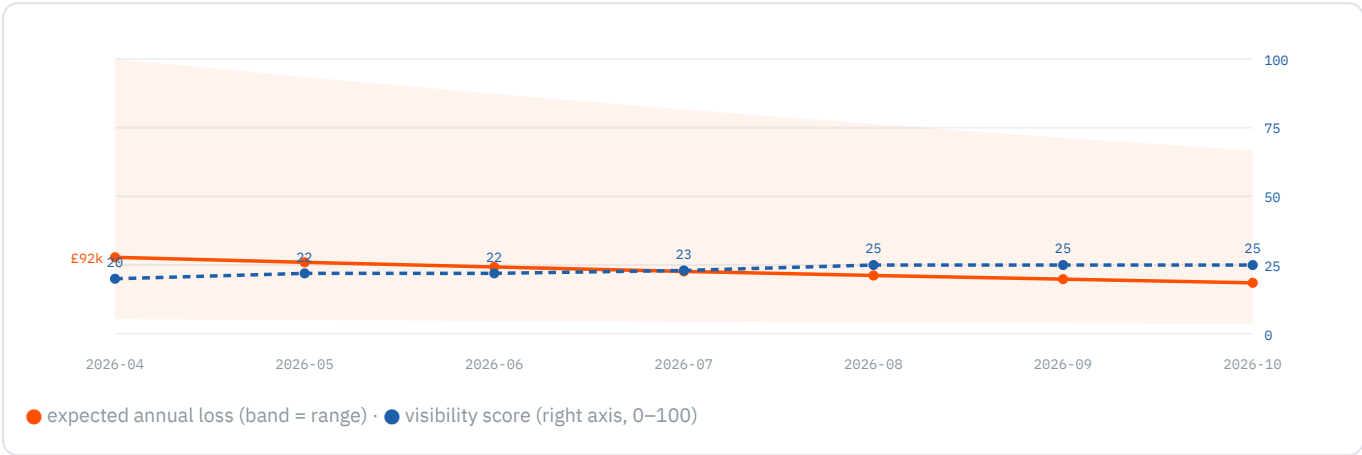
FIX	OWNER	TARGET	STATUS	VERIFICATION
Building Management Systems (BMS)	Cloud Platform Lead	2026-11-23	RISK ACCEPTED	next assessment
OT Remote Access Surfaces	IT Infrastructure Lead	2026-11-16	DONE	next assessment
API Keys	Cloud Platform Lead	2026-10-30	RISK ACCEPTED	next assessment
SD-WAN Infrastructure	—	—	RISK ACCEPTED	next assessment
Cloud Networking	—	—	DONE	next assessment
Exposed Services	—	—	IN PROGRESS	next assessment
OAuth Apps	Security Operations Manager	2026-10-23	OPEN	next assessment
Printers	Head of OT Engineering	2026-11-23	OPEN	next assessment
AI Agents	Identity & Access Lead	2026-12-24	OPEN	next assessment
Unintegrated M&A Infrastructure	Data Protection Officer	2026-11-09	OPEN	next assessment
SaaS Identities	Cloud Platform Lead	2027-01-07	OPEN	next assessment

18 of 82 fixes owned · 0 overdue · 2 done (0 verified closed). Each "done" is checked against the latest measured assessment — verified closed, or flagged if still open.

Programme = one control deployed across a layer for one gap type. Loss avoided = the programme's expected annual loss × (1 – residual ÷ measured exposure); closing a gap leaves ~15% exposure. Fix now = the programmes removing the first 50% of the removable loss; Next = to 80%. Routes = modelled attack routes with a hop this programme closes. Cumulative = share of expected annual loss removed by fixing to here. The order uses no prices; the cost of securing each layer is in section 6.

08 · TRAJECTORY

Are we buying down risk?



ASSESSMENT	EXPECTED ANNUAL LOSS	RANGE	VISIBILITY	BLIND SPOTS
2026-04-09	£92k	£18k-£333k	20	21
2026-05-09	£86k	£17k-£311k	22	16
2026-06-09	£81k	£16k-£291k	22	13
2026-07-09	£75k	£15k-£272k	23	11
2026-08-09	£71k	£14k-£254k	25	11
2026-09-08	£66k	£13k-£237k	25	11
2026-10-09	£62k	£12k-£222k	25	12

Exposure down 6.5% since last assessment — risk is being bought down.

APPENDIX · METHOD & SOURCES

How every number was produced

Exposure model

One organisation-level expected-annual-loss **anchor** is allocated across the measured gaps in proportion to each one's risk weight (frequency × measured exposure × reliance). Sightline's measurement decides *where* the loss sits; the anchor sets its *size*.

Anchor: revenue-at-risk: £180m × 0.034% (mean; median 0.015%) (range 0.0066%–0.12% of turnover). Expected annual loss is the **mean** — mean of a lognormal fitted to the row (median = central, 95th percentile = high); cyber loss is heavy-tailed, so the mean sits above the median (£28k, the conservative figure). Floor: CSBS 2024 floor — large (Open Government Licence v3.0) = £11k.

Loss-rate source

Agnostec starter loss-rate (real-loss derived) · release 2026-draft-v1 · utilities / medium (£100m–£1bn turnover).

Cyentia Institute, Information Risk Insights Study (IRIS) 2025

NetDiligence Cyber Claims Study (16th ed.)

UK DSIT Cyber Security Breaches Survey 2025 (UK context only; survey-based)

- US-weighted source data; apply UK calibration when a UK/EU-specific dataset is licensed
- central is median-anchored (conservative); 'high' carries the heavy tail (IRIS 95th loss ~100%+ of turnover for small firms)
- micro/small bands carry the highest uncertainty (source data groups sub-£40m coarsely)
- STARTER fallback only — the engine prefers the Agnostec internal dataset, then a licensed feed, above this

Generated 12 October 2026 at 14:46 (UK time) from assessment A-00050

Frequency

VCDB-derived relative shape (10047 incidents, 1971–2026) — absolute level anchored, all-sectors — CC BY-SA 4.0.

Visibility states

MEASURED owned & observed · **BLIND** owned, not observed · **SHADOW** observed, not owned. Total absence of evidence for a category is reported as a gap, never as clean.

Attack routes

Routes over MEASURED blind/shadow surfaces along a documented standard-attack progression model. Shows where blindness would let an attacker move undetected — not a prediction or a specific exploit chain.

Data handling

Sightline processes only tokenised, counted data exported by SILO on Demo — Sightline's own machines; names resolve only in SILO with the customer's key. Processed and stored in the UK (OVHcloud London).