

SOLUTION SCENARIO / AS OF 2026-10-02

A 25-user controlled-data program, with a maintained operating rhythm

Small team. Significant obligations. A program people can operate.

ILLUSTRATIVE / PROPOSED SELECTIONS / MODELED FINANCIAL RESULTS
Every selection, count and cost in this brief is illustrative. No actual customer result is represented.

Scenario and intended outcome

ENVIRONMENT Illustrative 25-user defense supplier with CDI/CUI and potential ITAR obligations. Contract, data classification and personnel eligibility have not been determined.	OBJECTIVE Connect supported IT, the required control baseline, responsible owners and recurring evidence without buying overlapping tools for every task.
SCOPE Governance, evidence coordination and a representative logging pilot. The complete controlled-data platform and assessment are separate decisions.	
MODEL BOUNDARY Governance/evidence/logging component only; this is not the \$7,625 partial managed-IT-plus-governance budget or a full compliance quote.	

A repeatable selection method

START WITH THE REQUIREMENT Map the business workflow, data classification, integrations, scale, recovery objectives, operator skills and support hours. Treat eligibility, security and mandatory features as pass/fail gates before scoring price.	COMPARE SUITABLE CANDIDATES For candidates that pass the gates, score functional fit 30%, operational maintainability 25%, integration and data portability 20%, three-year total cost 15%, and supplier/support resilience 10%. These are proposed weights, not completed vendor test results.	PROVE THE CHOICE Run a representative pilot, negative tests and recovery exercise. Price hosting, retention, patching, engineering, support, training and exit. A lower license bill wins only when the complete solution meets the requirement.
---	---	--

Proposed selections and alternatives

Illustrative options for evaluation; selection does not represent a completed vendor test or an actual quote.

FIRST, PASS THE GATES

Map the business workflow, data classification, integrations, scale, recovery objectives, operator skills and support hours. Treat eligibility, security and mandatory features as pass/fail gates before scoring price.

PROPOSED SCORING WEIGHTS AFTER THE PASS/FAIL GATES

For candidates that pass the gates, score functional fit 30%, operational maintainability 25%, integration and data portability 20%, three-year total cost 15%, and supplier/support resilience 10%. These are proposed weights, not completed vendor test results.

PROPOSED DIRECTION	ALTERNATIVE TO TEST
Proposed: retain the eligible identity and endpoint platform Use the customer's approved directory, endpoint protection and data boundary. Confirm the actual contract and platform eligibility first.	A commercial regulated platform may be the best fit when personnel, cryptographic, hosting or contractual requirements rule out an ordinary deployment.
PROPOSED DIRECTION	ALTERNATIVE TO TEST
Proposed: Windows WEF/WEC and a scoped Wazuh pilot Reuse built-in Windows event collection; evaluate open-source analysis for the approved event subset. Preserve source identity and test ingestion end to end.	Compare the existing commercial SIEM or managed offering against retention, investigation, support and eligibility needs. WEC is a Windows capability, not open-source software; Windows licenses remain.
PROPOSED DIRECTION	ALTERNATIVE TO TEST
Proposed: controlled evidence index and recurring reviews Assign control owners, evidence links, remediation status and review dates. Keep sensitive content in the approved customer boundary.	A commercial GRC platform is preferred when workflow, assurance integrations or scale justify it. An index alone does not implement or validate controls.

PROOF BEFORE CHOICE

Run a representative pilot, negative tests and recovery exercise. Price hosting, retention, patching, engineering, support, training and exit. A lower license bill wins only when the complete solution meets the requirement.

Architecture flow and delivery path

The sequence below follows the supplied scenario flow and implementation stages.

Architecture flow

01**Obligations -> boundary**

The sponsor approves clauses, framework revision, data paths, people, suppliers and support locations.

02**Systems -> evidence**

Approved systems provide scoped events and control evidence; the program tracks accountable owners and unresolved gaps.

03**Evidence -> decisions**

Phantom readiness work examines the scoped evidence and presents funded actions. Formal assessment and contractual acceptance follow the applicable authority.

Implementation stages

01 Discover and approve	Interview the sponsor and data owners; map obligations and actual systems. Stop if the support or hosting boundary is not eligible.
02 Design and pilot	Choose one representative workflow and logging source. Define retention, access, incident reporting and safe test data.
03 Roll out in stages	Deploy approved changes within maintenance windows; retain configuration and collector rollback. Do not route restricted data into a general support queue.
04 Validate and hand off	Rehearse an access change, evidence retrieval, collector outage and reporting tabletop. Assign monthly checks and corrective actions.

Acceptance and operating handoff

Acceptance evidence is scoped to the illustrative component described in this brief.

Acceptance checks

01

Acceptance check 1

Owner approves the contractual baseline and data/support boundary.

02

Acceptance check 2

Approved access succeeds; unauthorized and departed access fails.

03

Acceptance check 3

A test event retains originating identity, reaches the agreed destination and exposes a collector outage.

04

Acceptance check 4

Evidence is retrievable by the authorized reviewer; gaps remain visible without claiming a passing assessment.

Common handoff

01

Handoff 1

Customer owns approvals and business priorities; L8DT owns only the operating tasks and access authority in the signed schedule.

02

Handoff 2

Deliver versioned configuration, asset/data-flow registers, escalation and recovery runbooks, license obligations, known gaps and an acceptance record.

03

Handoff 3

Rehearse the operator workflow and restore before acceptance. Record owners, backup owners, training attendance, support hours and supplier escalation.

04

Handoff 4

Review coverage and evidence monthly; revisit capacity and access quarterly. Define export, credential removal and retention at termination.

36-month economics

Synthetic scenario inputs and calculated model outputs. These values are not a quote or realized savings.

Monthly assumptions and setup

Input	Illustrative commercial comparator	Illustrative L8DT model
One-time setup	\$18,000	\$15,000
License / month	\$900	\$300
Infrastructure / month	\$300	\$450
Service / month	\$3,000	\$2,500
Monthly cash total	\$4,200	\$3,250
Customer effort / month	8 hours	12 hours
Customer hourly value	\$65	\$65
Customer effort value / month	\$520	\$780

Calculated totals across 36 months

36-month total	Commercial comparator	L8DT model
Cash TCO (setup + monthly cash)	\$169,200	\$132,000
Customer-effort value	\$18,720	\$28,080
Economic TCO (cash + customer effort)	\$187,920	\$160,080

Modeled comparison outputs

NET CASH AVOIDANCE +\$37,200	COST AVOIDANCE 21.99%	CASH ROI 28.18%
ECONOMIC BENEFIT +\$27,840	PRETAX PROFIT DELTA: YEAR 1 / STEADY Y1 +\$14,400 steady +\$11,400	PAYBACK 0 months
L8DT EXTRA CUSTOMER TIME / MONTH 4 hours	SENSITIVITY ADD-ON / MONTH \$750	SENSITIVITY NET CASH AVOIDANCE +\$10,200

Model definitions, boundaries and references

Use the links and source notes for review. Public destination routes are targets; deployment was not verified for this package.

Definitions: cost avoidance = net cash avoidance / commercial 36-month cash TCO; cash ROI = net cash avoidance / proposed L8DT 36-month cash TCO. Economic benefit = commercial economic TCO minus L8DT economic TCO; economic TCO adds customer effort valued at the stated hourly input. Valued time is not payroll saving. Sensitivity applies the stated additional monthly L8DT operating cost for all 36 months.

REALIZED OUTCOMES

Realized ROI: NOT PROVIDED | Realized profit: NOT PROVIDED. These are not provided as customer results.

INTERPRETATION LIMIT

Illustrative scenario only. Proposed selections, input costs and modeled values are not actual customer results, completed vendor test results, or supplier quotes.

HYPOTHETICAL PROFIT-DELTA ASSUMPTION

Year-one pretax profit delta uses the modeled recurring cash difference less any incremental setup; steady-year delta uses 12 times the recurring cash difference. The model assumes costs are recognized as operating expenses with equal revenue and other costs. Capitalization, depreciation and tax treatment can differ.

Out of scope for this model

Ordinary managed IT, eligible CUI storage/cloud, restricted 24/7 staffing, remediation, assessor fees, legal/export review, taxes and hardware are excluded equally from this component model. No compliance score or certification is predicted.

WHAT TO PROVE AND PRICE

Run a representative pilot, negative tests and recovery exercise. Price hosting, retention, patching, engineering, support, training and exit. A lower license bill wins only when the complete solution meets the requirement.

Official project and product references

Microsoft Windows Event Forwarding

learn.microsoft.com

Wazuh project

wazuh.com

Source data as of 2026-10-02.

Related L8DT destinations

Experience story

</experience/controlled-data-25/>

Solution detail

</solutions/controlled-data-25/>

Website: <https://www.layer8defensetechnologies.com/>