Guide 7

The CISO's Guide to Vendor Rationalisation: When More Tools Means Less Security

A structured methodology for evaluating, removing and consolidating security tools, with a business case template.

Gadget Access Resources | April 2026 | Five-minute read

Header image: Vendor rationalisation is not fewer boxes on a diagram. It is clearer security decision-making.

Core argument

A tool that cannot generate a better decision is not a security investment. It is telemetry with a maintenance bill.

The vendor sprawl trap

Every security tool in your environment probably had a good reason for arriving. A breach, an audit finding, a board question, a new framework, a cloud migration, a vendor breakfast with suspiciously good coffee. The problem is not that the purchase was irrational. The problem is that nobody was given the job of making the stack rational again.

Security tools do not merely consume licence dollars. They consume attention, architecture capacity, analyst muscle memory, integration budgets, onboarding time, storage, support tickets, procurement cycles and scarce executive patience. A control that works in a lab but sits outside the SOC workflow is not a control. It is an expensive ornament with alerts.

Recent industry data backs what many CISOs already know. Cisco's 2025 Global State of Security research reported that 78 percent of security tools are dispersed or disconnected, 59 percent of teams identify tool maintenance as the main source of inefficiency, and 57 percent lose investigation time to data management gaps. Palo Alto Networks' 2025 cloud security research found organisations managing an average of 17 cloud

security tools from five vendors, with 97 percent prioritising consolidation. IBM's 2025 Cost of a Data Breach report put the average breach cost at US$4.4 million and found extensive use of AI in security associated with US$1.9 million in savings compared with organisations that did not use those solutions.

In Australia, ASD's ACSC reported more than 1,200 cyber security incidents responded to in FY2024-25 and more than 1,700 proactive notifications to entities of potentially malicious cyber activity, an 83 percent increase on the previous year. This makes vendor rationalisation more than procurement housekeeping. It is a cyber operating model issue. When the threat moves quickly and the team is already carrying more than it can process, more tools can quietly mean less security.

The false comfort of coverage

The typical stack map says everything is covered. Endpoint? Covered. Cloud? Covered. Vulnerability management? Covered. SIEM, SOAR, CTI, IAM, CASB, CNAPP, DSPM, GRC, MDM, email security, ticketing and reporting? Covered. The board sees a reassuring grid of green boxes.

The analyst sees something different. They see five dashboards describing the same suspicious identity pattern, two tools that disagree on asset ownership, a ticketing queue that has aged like unrefrigerated cheese, and a compliance team that still needs screenshots every quarter. The control exists, but the workflow does not.

The important CISO question is not, 'Do we have a tool for this?' It is, 'Can this capability produce a decision, at the right speed, with evidence we trust, in the hands of the person who can act?' If the answer is no, adding another platform is unlikely to fix it. It may simply add another version of reality.

This is where rationalisation requires courage. Some tools are genuinely critical. Some are under-used because they were poorly implemented. Some are duplicative. Some create valuable telemetry but should not be analyst-facing. Some are kept because everyone is afraid to remove them. The work is to separate technical sentiment from control value.

Figure 1. Rationalisation should preserve useful telemetry while reducing disconnected analyst workflows.

A better definition of rationalisation

Vendor rationalisation is not the hunt for one magical platform. Defence in depth still matters. Specialist tools still matter. Open standards still matter. The aim is to minimise needless complexity while preserving, and preferably improving, security outcomes.

The first principle is outcomes before logos. Map tools to control outcomes, not vendor categories. A vulnerability scanner, an attack surface tool and a CNAPP may all contribute to the same outcome: find, prioritise and remediate exploitable exposure. The second principle is data flow before dashboard count. A tool that feeds clean, timely evidence into your operating model may be more valuable than one with a brilliant console nobody opens.

The third principle is human workflow before feature lists. If analysts, engineers, risk owners and executives cannot use the output, the capability is not mature. The fourth is reinvestment before austerity. The best programs redirect savings into resilience: better logging, automation, engineering uplift, training, tabletop exercises, AI-assisted triage and continuous compliance.

The six-step method

Step 1 is to define the target security outcomes. Do not start with a spreadsheet of products. Start with the risk outcomes the business needs: protect critical services, detect identity compromise, reduce exploitable exposure, preserve evidence, meet regulatory obligations and recover fast. Anchor the outcomes to the frameworks that matter in your environment. For Australian organisations this commonly includes the Essential Eight, the ISM, PSPF, ISO 27001:2022 and NIST CSF 2.0. The NIST CSF 2.0 update is especially useful because its added Govern function makes cybersecurity strategy, decision-making and accountability explicit.

Step 2 is to build a security tool and telemetry register. Capture the vendor, product, owner, contract date, annual cost, support cost, deployment status, data sources, alert types, integrations, dashboards, playbooks, control mappings and evidence outputs. Then add the awkward but important questions. Who actually uses it? What would break if it vanished? Is the same telemetry already collected elsewhere? What evidence does it produce for auditors? What data does it send offshore? Does it help the SOC at 2:17 am on a Sunday, or just the renewal deck?

Step 3 is to score value, drag and removal risk. Control value asks whether the tool materially reduces risk or improves assurance. Operational drag measures how much maintenance, tuning, storage, integration work and specialist knowledge it consumes. Removal risk considers what coverage, legal obligation, contractual constraint or recovery option would be lost. The strongest candidates for retirement have low control value, high operational drag and low removal risk. The most important tools often have high control value and high drag, which means they need integration, automation or a replacement strategy rather than a sudden axe.

Step 4 is to choose the rationalisation pattern. Retain tools that are strategic and working. Retire tools that are redundant or unused. Replace tools where the capability is needed but the implementation is not sustainable. Integrate tools that generate useful telemetry but should not force another analyst workflow. Consolidate capabilities where one platform can credibly cover several outcomes. Quarantine legacy tools where removal is risky but continued expansion would be worse.

Step 5 is to pilot safely. Tool removal should be treated like change to a production control, not a procurement tidying exercise. Run parallel monitoring, preserve data retention, validate detection coverage, test playbooks, and define rollback criteria. The pilot should prove that the target state maintains or improves control coverage before savings are booked.

Step 6 is to convert savings into operating leverage. The goal is not just fewer invoices. It is a faster, clearer and more defensible security function. The best use of savings is usually boring in the most wonderful way: better log

coverage, cleaner asset data, playbook automation, improved vulnerability remediation, reusable compliance evidence, analyst training and executive reporting that does not need translation by three engineers and a poet.

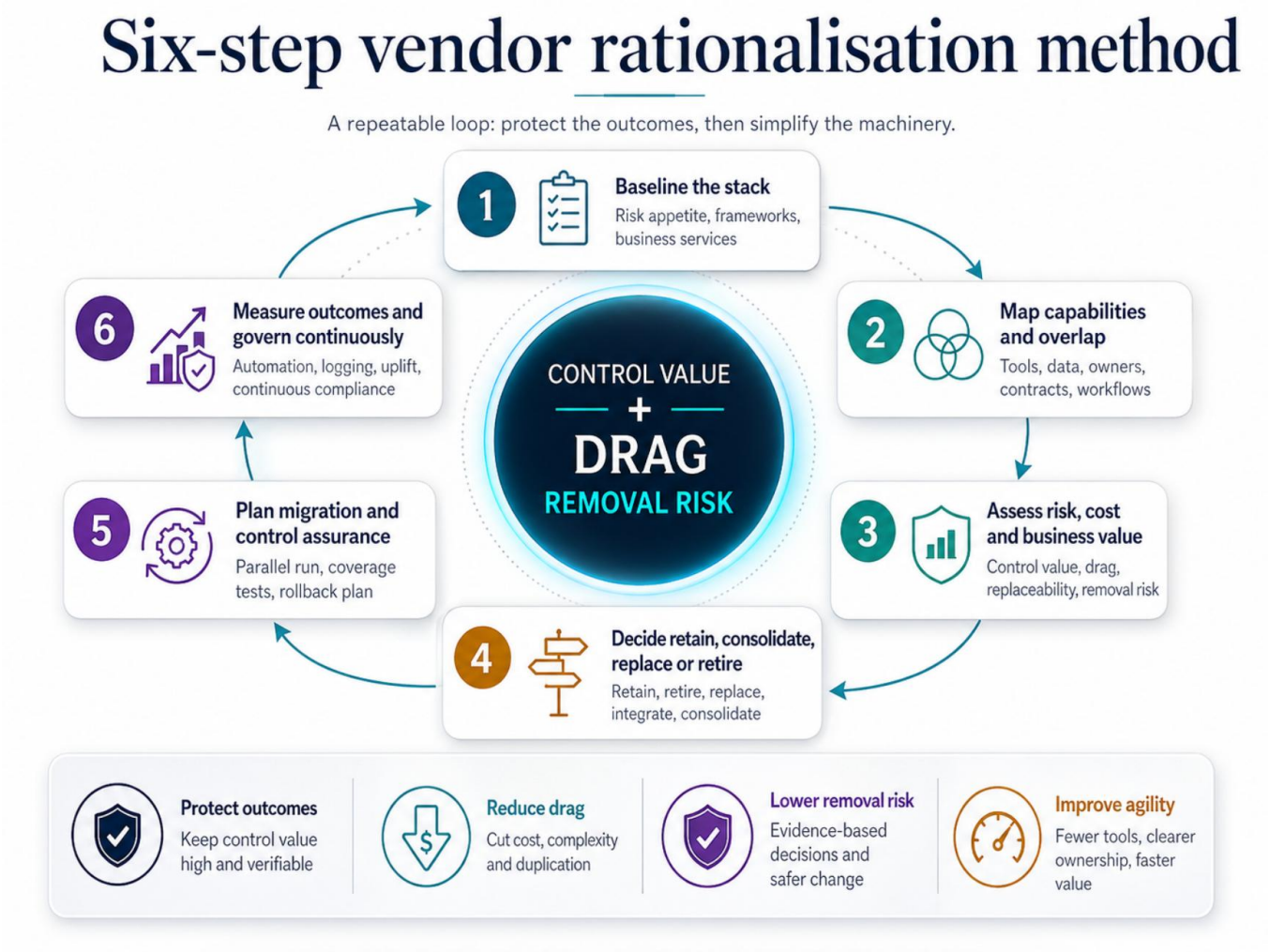

Figure 2. A repeatable rationalisation method balances control value, operating drag and removal risk.

Where AI changes the calculus

AI is changing both sides of the security equation. Attackers gain speed, scale and targeting precision. Defenders gain the ability to classify, correlate, summarise and respond at machine speed, provided the operating model is clean enough for AI to help rather than hallucinate its way through a junk drawer.

Anthropic's Project Glasswing is a useful signal of where the market is heading. Anthropic says selected partners receive access to Claude Mythos Preview to find and fix vulnerabilities or weaknesses in foundational systems, including tasks such as local vulnerability detection, black box testing of binaries, endpoint security and penetration testing. Whether a CISO sees this as exciting, terrifying or both, the implication is clear: vulnerability discovery and exploit analysis are becoming faster. Patch readiness, prioritisation and evidence-based decision-making need to keep up.

This is why vendor rationalisation cannot stop at 'cut three tools and save money'. It must create a platform for better decisions. CiBRAI's value proposition aligns with this need: bring endpoint, cloud, identity and network signals into one operational view, use sovereign agentic AI as an always-on analyst layer, group related activity, add business context, guide playbooks and produce clear audit trails. That is not rationalisation by deletion. It is rationalisation by design.

The Continuous Compliance connection

Compliance is often where tool sprawl hides. One product stores vulnerability data, another stores exceptions, a third stores audit evidence, and a fourth sends executive charts that are just optimistic enough to start an argument. The result is a control environment that is expensive to run and hard to prove.

Gadget Access' Continuous Compliance framework approaches this differently. It treats control evidence as a living operational product, not a quarterly archaeological dig. Rationalisation should therefore ask a simple question of every retained capability: can it produce reusable evidence for the control outcomes we report against? If not, can CiBRAI or another integration layer collect, normalise and preserve that evidence without forcing another manual process?

This matters for SMEs, enterprises and government agencies alike. The Essential Eight provides a baseline designed to make compromise harder. The ISM gives risk-based guidance for IT and OT systems. PSPF Release 2025 prescribes what Australian Government entities must do to protect people, information and resources. A rationalised stack should make these obligations easier to operate, not just easier to describe in a policy.

The decision rules

A simple rule helps: no tool should be retained unless it clearly improves one of three things. It must improve risk reduction, operational efficiency or defensible assurance. Ideally it improves two. If it improves none, it is a hobby with a purchase order.

A second rule is to reduce analyst-facing surfaces before reducing data sources. Logs, telemetry and context are valuable. Endless dashboards are not. In many environments the winning move is to keep the useful sensor, retire the console, and bring the evidence into a shared operating model. This is where a platform approach can beat a procurement-only consolidation program.

A third rule is to make removal observable. If a control is decommissioned and nobody can prove detection, response, evidence and reporting were preserved, the program has created risk even if the spreadsheet looks better. Rationalisation should leave a paper trail strong enough for the board, the auditor and the incident commander.

Rationalisation scorecard

Use a simple 1 to 5 scoring model to bring architecture, operations, risk and finance into the same conversation. The score is not a substitute for judgement. It is a way to make judgement visible.

Criterion	Question	Scoring guide
Control value	Does it materially reduce risk, improve detection, improve response or produce required evidence?	1 = unclear value, 5 = critical control
Operational drag	How much admin, tuning, specialist training, storage, integration and renewal effort does it consume?	1 = low drag, 5 = high drag
Replaceability	Can the function be absorbed by another retained capability or by an integration layer?	1 = hard to replace, 5 = easy to replace
Removal risk	Would removal create unacceptable detection, legal, audit, resilience or contractual risk?	1 = low risk, 5 = high risk

Criterion	Question	Scoring guide
Strategic fit	Does the tool align with target architecture, data sovereignty, AI strategy and operating model?	1 = poor fit, 5 = strong fit
Evidence value	Does it generate reliable evidence for Essential Eight, ISM, PSPF, ISO 27001, NIST or internal controls?	1 = weak evidence, 5 = reusable evidence

Closing thought

The next generation of cybersecurity will not be won by the team with the most portals. It will be won by the team with the clearest operating model, the cleanest evidence, the fastest decision loops and the best use of automation. Vendor rationalisation is one of the most practical ways to get there.

For Gadget Access, this is not just a cost exercise. It is a way to help Australian organisations build cyber programs that are leaner, more accountable and more resilient. CiBRAI extends that idea into daily operations by connecting the tools that still matter, reducing noise, guiding investigations and keeping compliance evidence alive. Less can absolutely be more, but only when less is engineered.

Business case template

Use this section as a reusable board and executive template. It works best when the CISO, CFO, procurement lead, security architect and risk owner complete it together. The goal is to show that the program saves money and improves measurable control outcomes, not merely that it reduces the number of suppliers.

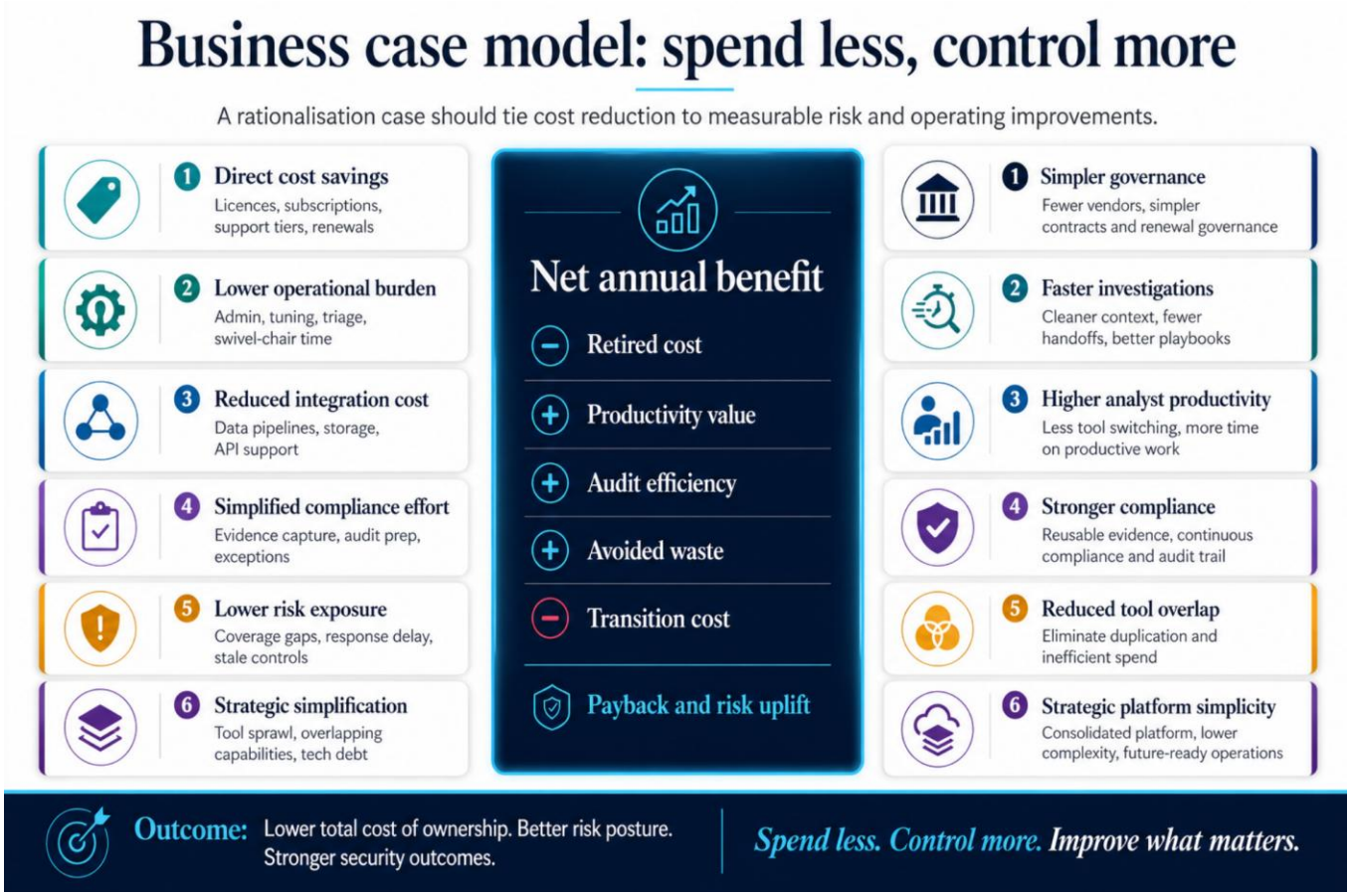

Figure 3. The business case should convert tool consolidation into financial value, operating leverage and defensible assurance.

Business case input table

Component	What to calculate	Evidence	Owner
Current annual tool spend	Licences, cloud consumption, support, managed services and unavoidable renewal commitments.	Finance export, contracts register, procurement records	CISO + CFO
Operational labour drag	Hours spent on tool administration, rule tuning, integration maintenance, alert triage and manual evidence collection.	Timesheets, SOC estimates, engineering backlog, audit prep logs	Security operations
Control overlap	Capabilities that duplicate the same outcome, produce the same telemetry or compete for the same analyst workflow.	Tool register, control mappings, telemetry map	Security architect
Target-state design	Retain, retire, replace, integrate, consolidate or quarantine decisions, with required guardrails.	Architecture decision record, risk assessment, pilot plan	CISO + architecture

Component	What to calculate	Evidence	Owner
Quantified benefits	Retired cost + avoided renewal + productivity value + audit efficiency + reduced integration cost.	Benefit model, vendor quotes, baseline hours	CISO + finance
Implementation cost	Migration, integration, training, parallel run, data retention, exit fees and change management.	Project estimate, vendor transition plan, legal review	Program manager
Risk controls	Coverage tests, rollback criteria, data retention validation, detection mapping and executive risk acceptance.	Test evidence, risk register, incident simulation results	Risk owner
Decision requested	Funding, contract changes, decommissioning approval, target architecture endorsement and timeline.	One-page executive brief	Executive sponsor

Calculation model

Metric	Formula or working assumption
Annual licence saving	Sum of retired tools + avoided renewals - incremental target platform cost
Productivity value	Hours saved per week × loaded hourly rate × 52
Incident response value	Incidents per year × time saved per incident × loaded hourly rate, plus any agreed downtime impact model
Compliance value	Assessment hours saved × assessments per year × loaded hourly rate, plus reduced external audit support if defensible
Net annual benefit	Licence saving + productivity value + incident response value + compliance value - annual target-state operating cost
Payback period	Implementation cost ÷ net annual benefit

Guardrail

Do not claim risk reduction simply because cost has fallen. Claim risk reduction only where detection coverage, response speed, evidence quality or remediation throughput has measurably improved.

One-page executive template

Field	Draft text
Problem statement	We operate [number] security tools across [number] vendors. [number] tools overlap, [number] are under-used and [number] require manual evidence or analyst handoff.
Risk statement	Current complexity creates [specific risk]: delayed investigation, duplicated alerts, unclear ownership, audit effort, data gaps or renewal exposure.
Target state	Retain [tools], integrate [tools], retire [tools], replace [tools] and use [CiBRAI or target operating layer] to provide unified incident view, guided playbooks and continuous evidence.

Financial case	Net annual benefit is estimated at [$value], with payback in [months]. Benefits include licence reduction, productivity improvement and compliance effort reduction.
Control assurance	Detection coverage, retention, response playbooks and evidence mapping will be validated against [Essential Eight, ISM, PSPF, ISO 27001, NIST CSF or internal controls].
Decision required	Approve target architecture, transition funding, contract changes and controlled decommissioning plan by [date].

Selected references

Australian Cyber Security Centre. Annual Cyber Threat Report 2024-2025.

Australian Cyber Security Centre. Essential Eight.

Australian Signals Directorate. Information Security Manual.

Australian Government. Protective Security Policy Framework Release 2025.

Anthropic. Project Glasswing: Securing critical software for the AI era.

Cisco. Global State of Security Report, 2025.

IBM. Cost of a Data Breach Report 2025.

NIST. Cybersecurity Framework 2.0 release.

Palo Alto Networks. State of Cloud Security Report 2025 insights.

CiBRAI. Unified Cyber Security Platform with AI.

Image assets: The header and diagrams in this document were created as bespoke Gadget Access article assets for this guide and are included separately in the companion asset pack.