APTO SOLUTIONS

WHITEPAPER

Assess, Optimise, Operate

The Splunk Value Realisation Playbook

A practical, three-stage framework for turning SIEM and observability spend into measurable business value — from maturity assessment through cost optimisation to sustainable managed operation.

Published by Apto Solutions · aptosolutions.co.uk

ISO 27001 Certified · Splunk Partnerverse · Cribl Partner · Softcat Partner

Contents

Contents 1
Executive summary 2
1. The platform value problem 3
2. The Assess, Optimise, Operate loop 4
Why the order matters 5
3. Assess — know where you stand 5
3.1 The assessment portfolio 6
3.2 What you receive 8
4. Optimise — spend less, see more, operate smarter 9
4.1 Three levers for cost reduction 10
4.2 Pipeline optimisation pays for itself 11
4.3 Platform-specific optimisation 12
5. Operate — sustain the gains, keep the value climbing 13
Why a managed model matters 15
6. Case studies 15
6.1 £180K annual saving through pipeline engineering 16
6.2 SIEM assessment transforms security posture 16
7. The Splunk Value Realisation Playbook 17
From questions to action 18
Ready to take control of your Splunk investment? 18

Executive summary

Across every Splunk and observability conversation Apto has, the same question surfaces in different forms: is the platform actually delivering the value the business is paying for? Licence costs are climbing, detection coverage feels patchy, ingestion is growing faster than insight, and the people best placed to tune the estate are the hardest to hire and retain.

This whitepaper brings together two of Apto's core disciplines — Consulting & Assessment and Cost Optimisation — into a single, coherent playbook. The premise is simple: you cannot optimise what you have not assessed, and you cannot sustain optimisation without an operating model behind it. We call this the Assess, Optimise, Operate loop, and it is the path our clients use to realise the full value of Splunk, Sentinel, Datadog, Cribl and OpenTelemetry.

What you will get from this paper

- A clear framework for diagnosing where your Splunk and observability investment is actually delivering value — and where it is quietly leaking it.
- Four structured assessments that map platform maturity, use case effectiveness, data flows and operational readiness in two to four weeks.
- Three cost levers — licence optimisation, data volume reduction, and platform consolidation — that typically deliver 30-50% reduction in total spend with no loss of coverage.
- A worked pipeline example showing how a 100TB/day Splunk environment moved £324,000 of annual cost into a data lake while preserving every security-relevant event.
- A managed-service model that protects those gains against cost drift, skills-gap risk and ES rule rot.

1. The platform value problem

Splunk, Sentinel, Grafana, Datadog and their peers have become load-bearing infrastructure for modern security and operations. They also sit in the single most expensive line item in many technology budgets. In Apto's 2024-25 engagements, platform cost is the number one concern raised by CIOs, Heads of Cloud and SOC leaders — but it is rarely an isolated cost problem.

When we dig into the conversation, three connected themes come up again and again:

Theme 1 — Cost overruns and licence waste

Ingest-based licensing punishes growth. More data sources come online, ingestion volume grows, and licence costs follow. Teams are told to "cut ingestion" without visibility into what each gigabyte is actually worth, and so they either over-cut (creating security blind spots) or under-cut (missing renewal deadlines). In most environments we audit, 20 to 40 per cent of licensed capacity is underutilised and 30 to 50 per cent of ingested data is duplicated, low-value, or never queried.

Theme 2 — SOC modernisation and ES health

Enterprise Security deployments age quickly. Detection rules get written, then never reviewed. Data models drift. Notable events become noise. Analysts stop trusting the tool. The typical SOC we assess has detection coverage against only a fraction of the MITRE ATT&CK techniques relevant to its threat model, even though the technical capability to cover more is already licensed. The cost problem is really a value problem in disguise: the platform is not broken, it is untuned.

Theme 3 — Skills and sustainability

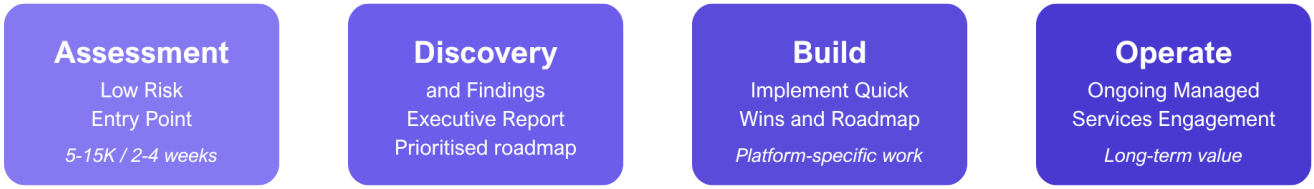
Splunk engineers, Cribl-literate pipeline specialists and content developers for ES are among the hardest technology roles to hire and retain in the UK market. Optimisation projects succeed, then quietly regress as the people who delivered them move on. Without a sustainable operating model, every cost saving is temporary.

This whitepaper is structured around the response Apto has built to those three themes — a three-stage loop that begins with honest assessment, moves into focused optimisation, and is sustained through a managed Operate service.

2. The Assess, Optimise, Operate loop

Apto's engagements are deliberately sequenced. Every project either starts in Assess or has an Assess equivalent built into its kick-off. Optimise turns assessment findings into delivered change. Operate sustains those changes and feeds new findings back into the next assessment cycle.

From Assessment to Operate: Your Success Journey



What Happens at Each Stage:

Assessment (Weeks 2-4)
Comprehensive platform audit.
Gap analysis against frameworks.
Executive summary and recommendations.

Discovery
Executive presentation.
Prioritised improvement roadmap.
Quick wins identified.

Build (Varies by scope)
Implement quick wins.
Platform optimisation.
Knowledge transfer.

Operate (Ongoing)
24/7 monitoring and alerting.
Proactive optimisation.
Continuous improvement.

The loop is intentionally lightweight at the entry point. A two-to-four-week assessment commits you to nothing beyond the findings themselves. In practice, 85 per cent of assessment clients move into Build (Optimise) or Operate engagements, because the assessment makes the business case impossible to ignore. But the option to take the deliverables to an internal team or alternative partner is always preserved.

Why the order matters

Skipping Assess is the single most expensive shortcut we see. Optimisation without a current-state baseline either cuts the wrong thing (creating security or observability gaps) or cannot prove its ROI (which makes the next optimisation harder to fund). Operate without Optimise first means a managed service team inherits the same waste and complexity the previous team struggled with — the run-rate cost just moves from one line of the budget to another.

Done in order, the three stages compound. Assessment findings quantify the prize. Optimisation delivers it quickly, with measurable ROI. Operate protects the gains and keeps discovering new ones — because Splunk environments drift the moment you stop paying attention.

3. Assess — know where you stand

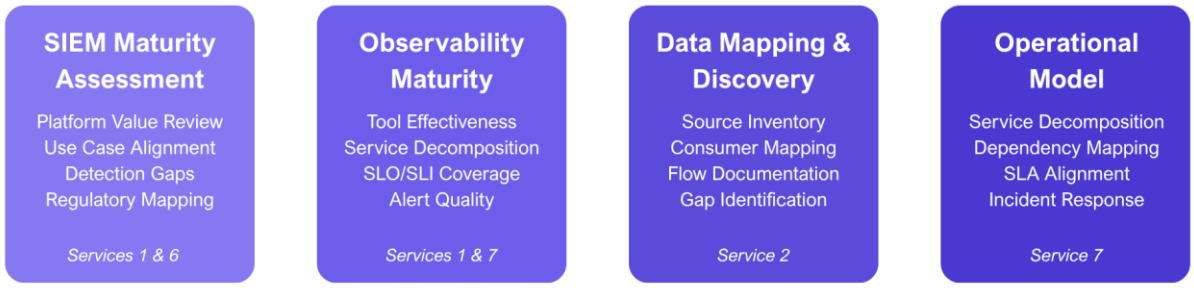
Most organisations do not know the true state of their platforms. They know something is not right: costs are climbing, alerts are noisy, dashboards are stale, or the team is stretched too thin. Without a structured assessment it is impossible to know where the real problems lie or which improvements will deliver the most value.

An Apto assessment is the fastest way to move from uncertainty to clarity. In two to four weeks, with zero disruption to production, we give you a complete picture of where you stand and a prioritised roadmap for where to go next.

3.1 The assessment portfolio

We offer four structured assessments, each targeting a specific domain. They can be run individually or combined for a comprehensive view across your entire platform landscape.

Assessment Portfolio



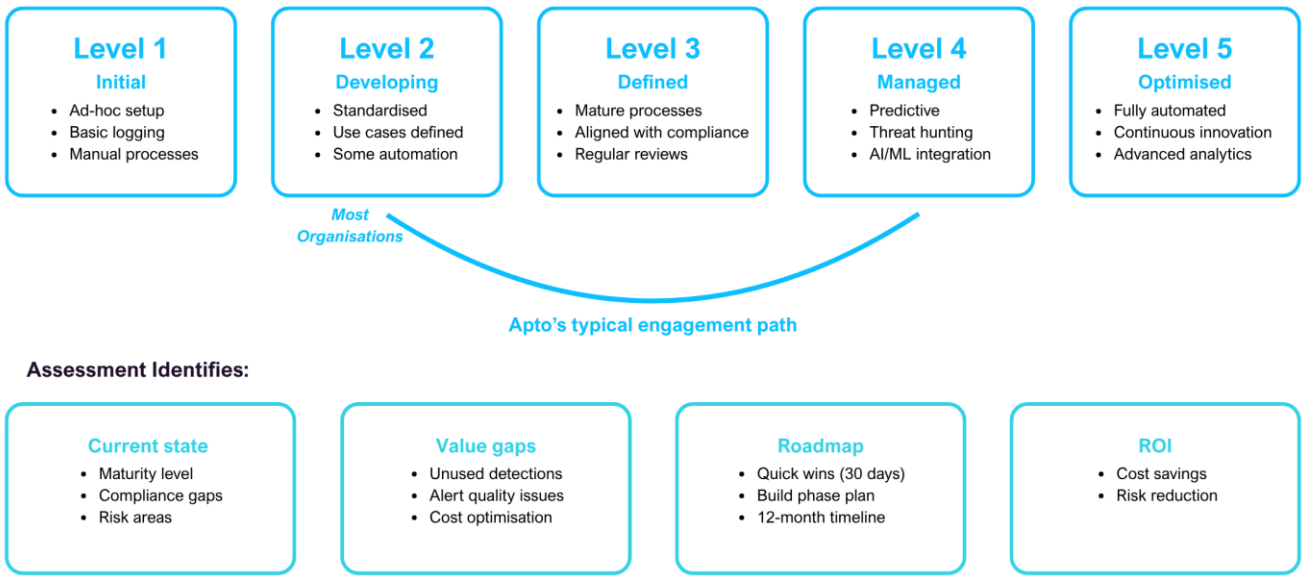
All assessments naturally feed into Build & Operate engagements

SIEM Maturity Assessment

Our most comprehensive assessment, combining platform value analysis with use case effectiveness review. We evaluate how your SIEM (Splunk, Sentinel, or other) is actually being used today, what security outcomes it supports, whether use cases align with your risk register and threat landscape, detection coverage against MITRE ATT&CK, regulatory alignment (NIST, ISO 27001, GDPR, PCI DSS), and whether cost and operational overhead are justified by the value delivered.

Sub-services included: threat model review, platform health check, use case gap analysis against MITRE ATT&CK, detection rule audit, data source quality assessment, licence utilisation review, and regulatory framework mapping.

SIEM Maturity Model: Where Are You Now?



Most organisations we assess sit at Level 2 (Developing) on the maturity model. They have a SIEM, some rules are in place, but detection coverage is patchy, many rules are outdated, and nobody is systematically reviewing effectiveness. The assessment identifies exactly where you are and maps the path to Level 4 or 5. For Splunk ES specifically, this is where the SOC modernisation conversation starts: tuning correlation searches, retiring redundant content, rebuilding risk-based alerting, and preparing the estate for SOAR integration.

Observability Maturity Assessment

Evaluates how effectively your monitoring tools are serving your engineering and operations teams. The assessment looks beyond whether tools are deployed to whether they are actually driving better reliability outcomes. We cover APM, infrastructure monitoring, log analytics and distributed tracing; service decomposition and dependency mapping; SLO/SLI maturity and error budget tracking; alert quality, noise levels, and escalation paths; dashboard relevance and usage; and tool sprawl and overlap across teams.

The output is a clear observability maturity score and a prioritised improvement roadmap that points directly into the Optimise stage.

Data Mapping & Discovery

A discovery exercise that maps all telemetry sources across applications, infrastructure, cloud, and security systems; who consumes each data source and for what purpose; current data flows and ingestion paths; gaps, overlaps and redundancies in collection; data quality, completeness and availability; and the cost implications of current data routing.

This is the critical bridge between understanding your current state and designing a target-state architecture. It provides the factual foundation for decisions about pipeline design, tool consolidation and cost optimisation. Most organisations are surprised by what they discover: duplicate data, sources nobody uses, and gaps that leave critical systems unmonitored.

Operational Model Assessment

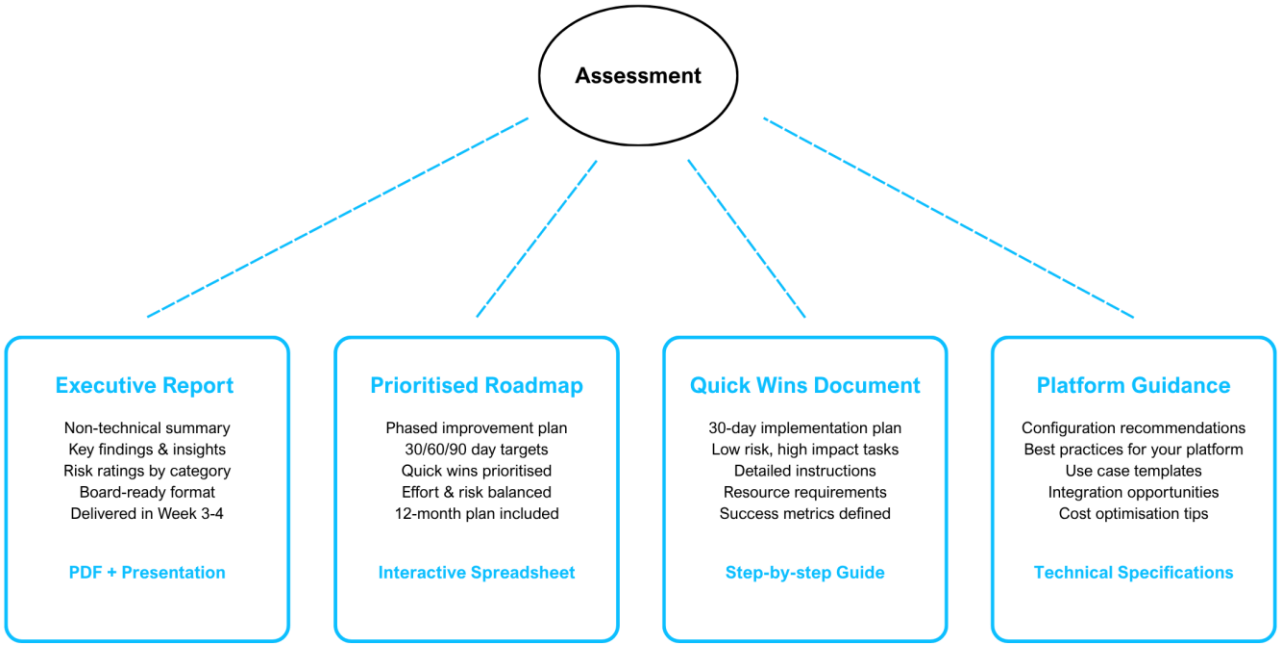
Designed for production monitoring teams responsible for ensuring IT platforms and applications are available, performant and reliable for end customers. We assess service decomposition into monitorable components; dependency mapping and potential points of failure; alignment of monitoring and alerting with customer-facing SLAs; alert quality, redundancy, and blind spots; incident detection, escalation, and response processes; and operational maturity against industry benchmarks.

The output identifies whether your monitoring is genuinely aligned with what matters to your customers, or whether it has drifted into monitoring infrastructure for its own sake.

3.2 What you receive

Every assessment produces a set of structured deliverables designed to be immediately actionable, whether you proceed with Apto or take the findings to your own team.

What You Receive: Assessment Deliverables



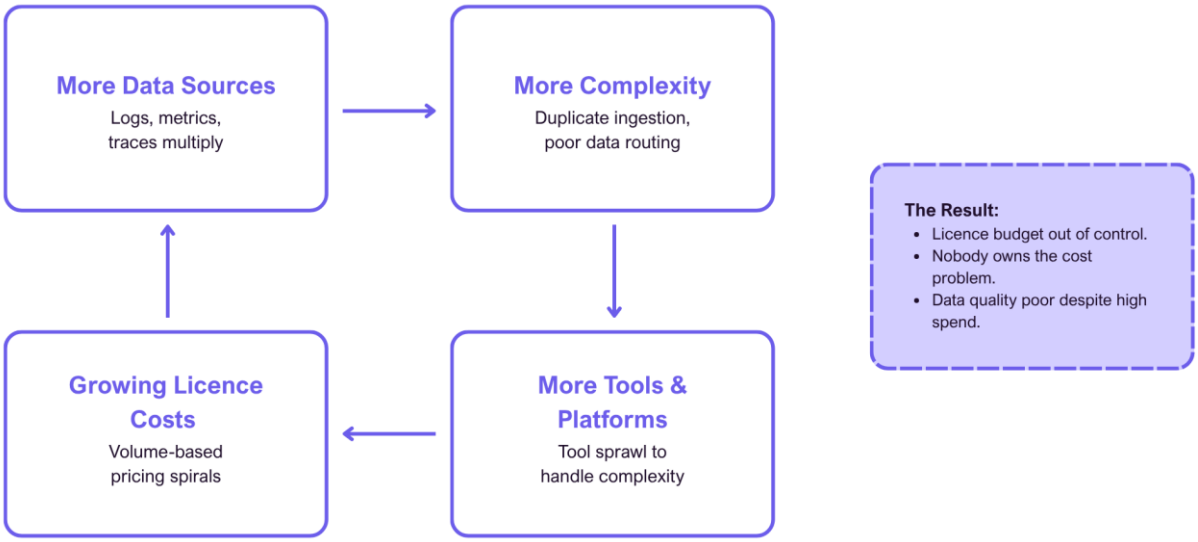
Bonus Delivarables: Cost-benefit analysis · Compliance mapping · ROI projections · Incident response review (where applicable)

Deliverable	What it contains
Executive report	Clear, jargon-free summary of findings for leadership and stakeholders. Includes maturity scoring, risk assessmentand strategic recommendations.
Prioritised roadmap	Sequenced improvement plan with estimated effort, impactand dependencies. Designed to deliver quick wins first while building toward long-term goals.
Quick wins	Immediate improvements that can be implemented in days, not weeks. Typically alert tuning, data source cleanup, licence right-sizing and retired ES content.
Platform recommendations	Specific, platform-level guidance for Splunk, Sentinel, Datadog, Cribl or OpenTelemetry. Includes configuration, architecture and operational recommendations.
Cost analysis	Detailed breakdown of current costs, identified savings opportunities and projected ROI from recommended improvements.

4. Optimise — spend less, see more, operate smarter

Assessment findings point to the prize. Optimise delivers it. Platform costs are the number one pain point in every Splunk, Sentinel and observability conversation we have, and costs have a tendency to spiral upward in a vicious cycle that feels impossible to escape.

The Cost Spiral



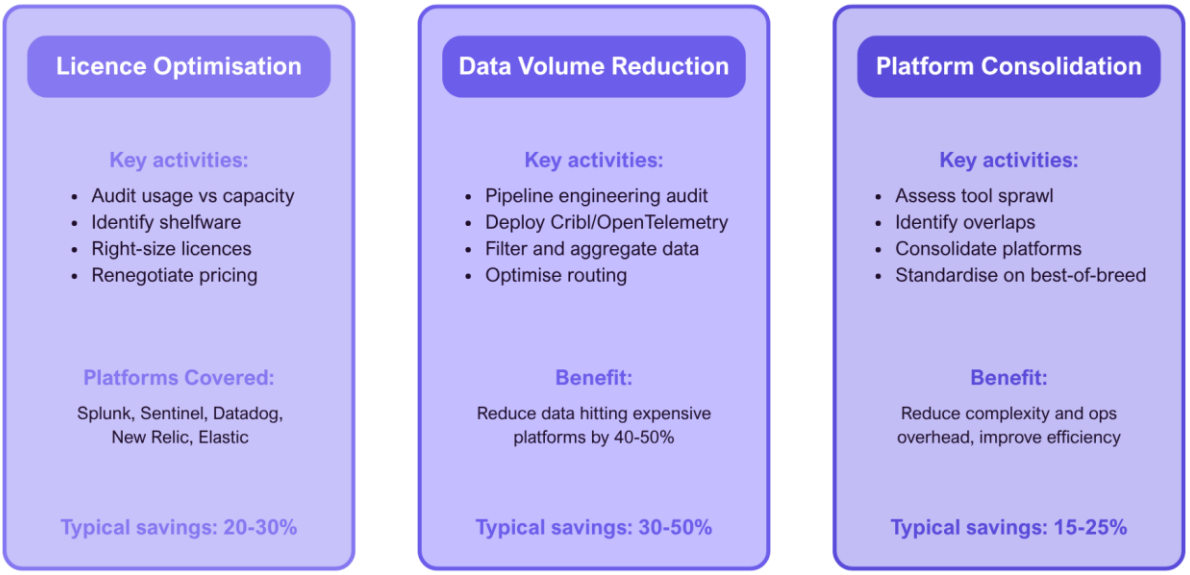
More data sources come online. Ingestion volumes grow. Licence costs increase. To manage the complexity, organisations add more tools. More tools mean more operational overhead, which requires more staff. And the cycle continues.

The root cause is almost always the same: there is no systematic approach to managing what data goes where, whether it is needed, and whether the cost is justified by the value it delivers. Most organisations are paying for data they do not use, tools that overlap, and licences that are not right-sized. The assessment stage quantifies the gap; the optimisation stage closes it.

4.1 Three levers for cost reduction

Apto approaches cost optimisation through three complementary levers. Used together, they typically deliver a 30 to 50 per cent reduction in total platform spend.

Three Levers of Cost Optimisation



Lever 1 — Licence optimisation

Most organisations are not using what they have already paid for. We audit licence utilisation across Splunk, Sentinel, Datadog, New Relic and other platforms to identify shelfware, over-provisioning and opportunities to right-size. This includes reviewing contract terms, identifying unused features, and helping with vendor renewal negotiations. This is where also, apto build a predictive model, asset input, sizing and licence forecasting. This enables far better assessment of platform costs in the future based on historical growth and events such as a mergers or cloud migration.

Typical findings: 20 to 40 per cent of licensed capacity is underutilised. Features purchased during initial deployment are never activated. Contract terms have not been reviewed since the original purchase. Multi-year commitments are locking in prices that no longer reflect market rates.

Lever 2 — Data volume reduction

This is the biggest lever for most organisations. SIEM and observability licences are typically priced on data ingestion volume. By introducing intelligent data pipelines using Cribl Stream or OpenTelemetry, we filter, deduplicate, route and tier data so that only high-value data reaches expensive platforms. Lower-value data is routed to cheaper storage like data lakes or archive.

Typical findings: 30 to 50 per cent of ingested data is duplicated, low-value or never queried. Verbose logging from development and staging environments is sent to production SIEM at full cost. Data that should be archived is being stored in hot, expensive tiers.

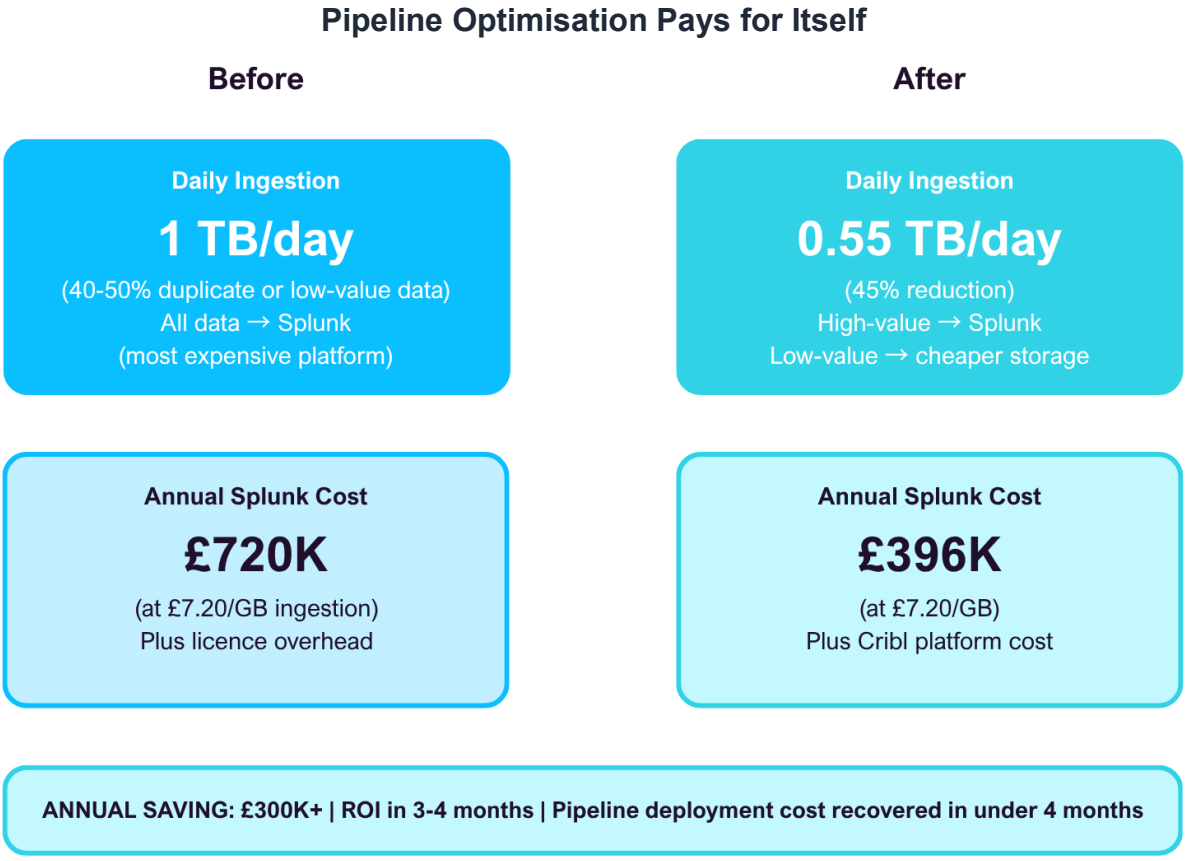
Lever 3 — Platform consolidation

Many organisations have accumulated overlapping tools across teams: one for security, one for infrastructure monitoring, one for APM. We assess tool overlap, identify consolidation opportunities and help rationalise the platform landscape. Fewer tools means lower licence

costs, reduced operational overhead and simpler data management — and it is often the consolidation conversation, not the licence conversation, that unlocks the biggest savings.

4.2 Pipeline optimisation pays for itself

Data pipeline engineering through Cribl, pipeline tooling or OpenTelemetry is the single most impactful cost optimisation technique available. By placing an intelligent routing layer between your data sources and your analytics platforms, you gain complete control over what data goes where and at what cost.



In the example above, a 100TB/day environment was spending £720,000 per year routing all data to an expensive SIEM tier. By introducing Cribl Stream as a routing layer, 45TB of lower-value data was redirected to a data lake at a fraction of the cost. The remaining 55TB of high-value security and operational data continued to the SIEM. Annual savings: £324,000, with no loss of security coverage.

The pipeline investment typically pays for itself within the first three to six months of operation. After that, the savings are pure cost reduction on an ongoing basis.

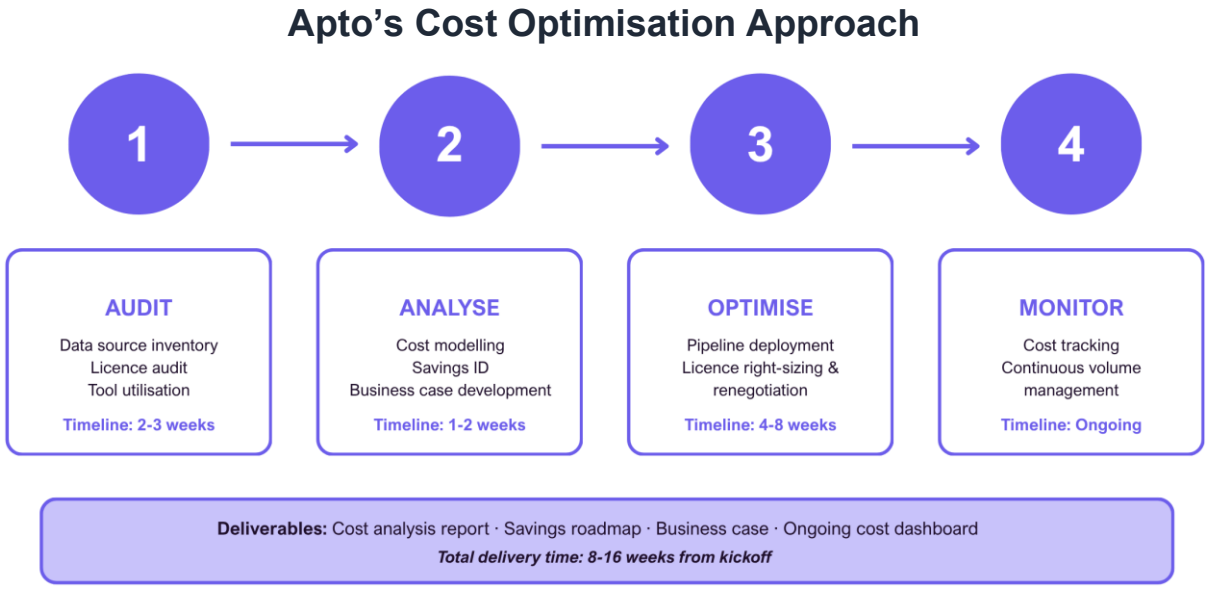
4.3 Platform-specific optimisation

Each platform has its own cost model and optimisation opportunities. Apto brings deep expertise across all major platforms and uses the right lever for each.

Platform	How Apto reduces cost
Splunk	Ingest-based licensing makes data volume control critical. We optimise through Cribl pipeline engineering, summary indexing, metrics store migration, search optimisation to reduce compute costs, and licence right-sizing. Partnerverse expertise means we understand Splunk pricing models intimately.
Sentinel	Pay-as-you-go Azure model means cost control is about data retention tiers, log analytics workspace optimisation, and commitment tier selection, lake alternatives. We help right-size Sentinel deployments and implement Basic, Analytics and Archive log-tier strategies. Pipeline data reduction.
Datadog	Per-host and per-metric pricing requires careful management of custom metrics, APM trace sampling rates and log volume. We optimise through metric cardinality reduction, intelligent sampling and removing unused integrations.
Cribl	Cribl is often the solution itself, not the cost problem. We help organisations deploy Cribl Stream to reduce ingestion costs across all downstream platforms. Pipeline engineering, data routing and format normalisation deliver ROI across the entire stack.
OpenTelemetry	As an open-source standard, OTel reduces vendor lock-in and allows flexible routing to any backend. We implement OTel Collector deployments that give organisations complete control over their data flow and cost allocation.

5. Operate — sustain the gains, keep the value climbing

Cost optimisation is not a one-off project. It requires an initial intensive review followed by ongoing monitoring and continuous improvement. Our four-stage process ensures you see quick wins fast while building sustainable long-term cost control — and it folds directly into the Operate managed service for clients who want to hand the run-state to us.



Audit (2-3 weeks)

We review licence utilisation, data ingestion patterns, tool overlap and contract terms. This produces a clear picture of where money is being wasted and where the biggest savings opportunities lie. Where the client has already run an Apto assessment, Audit reuses those findings and goes straight to the numbers.

Analyse (1-2 weeks)

We model the impact of different optimisation scenarios, quantify potential savings and build a business case with projected ROI. This includes pipeline design, licence right-sizing recommendations and consolidation options.

Optimise (4-8 weeks)

We implement the agreed changes: deploying pipelines, reconfiguring data routing, right-sizing licences and retiring redundant tools. Every change is validated to ensure no loss of security or observability coverage.

Monitor (ongoing)

Through our Operate service, we continuously monitor data volumes, licence utilisation and cost trends. We catch cost drift early and implement ongoing optimisations as your environment evolves. Operate also optionally owns ES content hygiene — detection rule

reviews, correlation search tuning, MITRE coverage mapping — so that the SOC modernisation work delivered in Optimise does not quietly decay.

Why a managed model matters

The single largest risk to any Splunk or observability optimisation is the skills gap. Splunk engineers, Cribl specialists and ES content developers are among the hardest technology hires in the UK. Apto's Operate service gives clients access to a bench of certified engineers on a predictable monthly commercial — removing the recruitment and retention risk while institutionalising the discipline that protects every pound of saving.

6. Case studies

6.1 £180K annual saving through pipeline engineering

Challenge. A UK enterprise client was facing a Splunk licence renewal with costs projected to increase by 35 per cent due to data volume growth. The security team had been told to cut ingestion, but had no visibility into what data was being sent or whether it was needed. Cutting the wrong data sources risked creating security blind spots.

Approach. Apto conducted a data mapping exercise and cost audit. We identified that 45 per cent of ingested data was either duplicated, verbose developer logging, or low-value network telemetry that was never queried. We deployed Cribl Stream as a data routing layer, implementing intelligent filtering, deduplication and tiered routing. High-value security data continued to Splunk; lower-value data was routed to S3 for long-term archive at a fraction of the cost.

Outcome. Splunk ingestion reduced by 45 per cent, saving £180,000 per year in licence costs. All security-relevant data was preserved with zero detection-coverage loss. The Cribl deployment paid for itself within four months. Data quality actually improved because deduplication and normalisation cleaned up inconsistent source formatting. The renewal was negotiated at a lower tier, locking in savings for three years.

6.2 SIEM assessment transforms security posture

Challenge. A UK organisation had invested heavily in Splunk Enterprise Security but was seeing diminishing returns. The SOC team was overwhelmed with alerts, detection rules had not been reviewed in over 18 months, and leadership had no clear picture of whether the SIEM was delivering value commensurate with its cost.

Assessment. Apto conducted a combined SIEM Maturity Assessment and Data Mapping exercise over three weeks. We reviewed all 240+ detection rules against the MITRE ATT&CK framework, mapped every data source and its ingestion path, and analysed licence utilisation patterns. The findings were clear: 60 per cent of detection rules were outdated or ineffective, 45 per cent of ingested data was low-value or duplicated, and detection coverage addressed only 28 per cent of relevant ATT&CK techniques.

Outcome. The assessment led directly to a Build engagement. Within four months, 140+ outdated rules were retired or rewritten, detection coverage increased to 72 per cent of relevant techniques, data ingestion was reduced by 40 per cent through pipeline optimisation, and annual licence costs were reduced by £95,000. The assessment paid for itself many times over — and the client subsequently moved detection engineering and content hygiene into Apto's Operate service to protect the gains.

Case study comparison

Dimension	Case study 1 — Pipeline	Case study 2 — ES Assessment
Entry stage	Optimise (renewal pressure)	Assess (effectiveness concern)
Primary lever	Data volume reduction	Use case & rule rationalisation
Annual cost saved	£180,000	£95,000
Coverage impact	Zero loss	28% → 72% MITRE coverage
Follow-on engagement	Operate — pipeline run state	Operate — ES content hygiene

7. The Splunk Value Realisation Playbook

Stripped to its essentials, the playbook is six questions. Anyone accountable for a Splunk or observability investment should be able to answer them in the next quarter; if they cannot, the assessment stage is the right next step.

- **1. Value.** Which user groups consume our Splunk data, and what business outcome does each group deliver from it?
- **2. Coverage.** What percentage of our relevant MITRE ATT&CK techniques are covered by active, tuned detections today?
- **3. Cost attribution.** Can we attribute licence cost to user groups, business units or use cases — and is each of those lines defensible?
- **4. Data hygiene.** What proportion of ingested data is duplicated, verbose or never queried, and how quickly could we remove it without losing coverage?
- **5. Tool overlap.** Where do Splunk, Sentinel, Datadog or others duplicate one another, and which platform is the strategic home for each use case?
- **6. Sustainability.** If the two people who know our Splunk estate best left tomorrow, how long would the gains we have made today survive?

From questions to action

Apto's model is designed to answer those six questions in order, quickly, and with measurable economic impact at every stage.

Stage	Typical duration & commitment	Typical economic outcome
Assess	2-4 weeks, fixed fee, zero production disruption	Quantified savings opportunity, maturity baseline, prioritised roadmap — deliverables usable with or without Apto
Optimise	4-8 weeks, outcome-priced	30-50% reduction in platform spend; pipeline, licence and consolidation changes delivered; ROI within 3-6 months
Operate	Ongoing managed service, monthly commercial	Continuous monitoring of cost drift, ES content hygiene, pipeline run state; eliminates skills-gap risk; protects and extends Optimise gains

Ready to take control of your Splunk investment?

If any of the six questions above feels uncomfortable to answer, that is the signal. An Apto assessment will give you the facts in weeks, not quarters — and the option, but never the obligation, to move straight into Optimise and Operate.

Book a free discovery call: aptosolutions.co.uk/contact

Learn more about our services: Consulting & Assessment · Cost Optimisation

About Apto Solutions

Apto Solutions is a UK-based specialist consultancy focused on Splunk, SIEM and observability platforms. We combine deep platform expertise with an outcomes-led commercial model, helping clients realise the full value of their investment through our Assess, Optimise and Operate services. We are ISO 27001 certified and partner with Splunk (Partnerverse), Cribl and Softcat.