dynatrace

Twelve tools and still flying blind

How to modernise to get more from your technology estate as AI advances and budgets shrink

Imagine for a moment…

"You open your dashboard while your coffee's brewing. It is July and everything is green. You scroll to the bottom showing agentic AI services and it's green too. Content, you close the laptop and think back to eighteen months ago when this would have been unthinkable."

The brief handed to every technology leader across the Australian Public Service makes this reality seem unachievable: find 5% efficiency savings[1], absorb the pay rise, manage with fewer people, implement AI responsibly, and do not let any critical services go down. That is not just a tough ask, it seems like a contradictory one.

This paper sets out a practical way to improve service delivery while reducing cost and position you for future innovation. Specifically:

- Why **tool sprawl** is the hidden cost nobody is auditing
- **Three strategies** enabled by a single platform to unify telemetry, reduce toil with answers, and advance automation and AI governance
- **A 90-day plan** you can start without a disruptive retooling event

SECTION ONE

The drain nobody's talking about

Most government technology leaders know their estates are complex. What is less visible is how much of their budget and their people's time is consumed by managing that complexity, rather than delivering and enhancing services to the public.

The average enterprise organisation runs **12** separate observability and monitoring tools.

— Dynatrace State of Observability for Public Sector Organizations 2024

Twelve! Each with its own licensing cost, skillset requirements, alert stream, and vendor relationship. Ninety-seven percent of those same leaders say their technology stack complexity has increased in the past 12 months. Eighty-seven percent say their environments now produce more data than their teams can meaningfully process.[2]

Meanwhile, the threat environment continues to intensify. ASD's ACSC recorded over 1,200 cybersecurity incidents in 2024-25, an 11% increase year on year, with DDoS attacks up 280%.[3]

87% say their environments produce more data than their teams can meaningfully process.

— Dynatrace State of Observability for Public Sector Organizations 2024

This is the hidden tax on government IT. It does not appear as a line item, but it shows up in every incident bridge call, every manual correlation exercise, every alert storm that burns out an already-stretched team.

It compounds when people leave. When an experienced engineer leaves, they often take with them institutional knowledge that is critical to the resilience of digital services, such as which alert matters and which dashboard reflects reality.

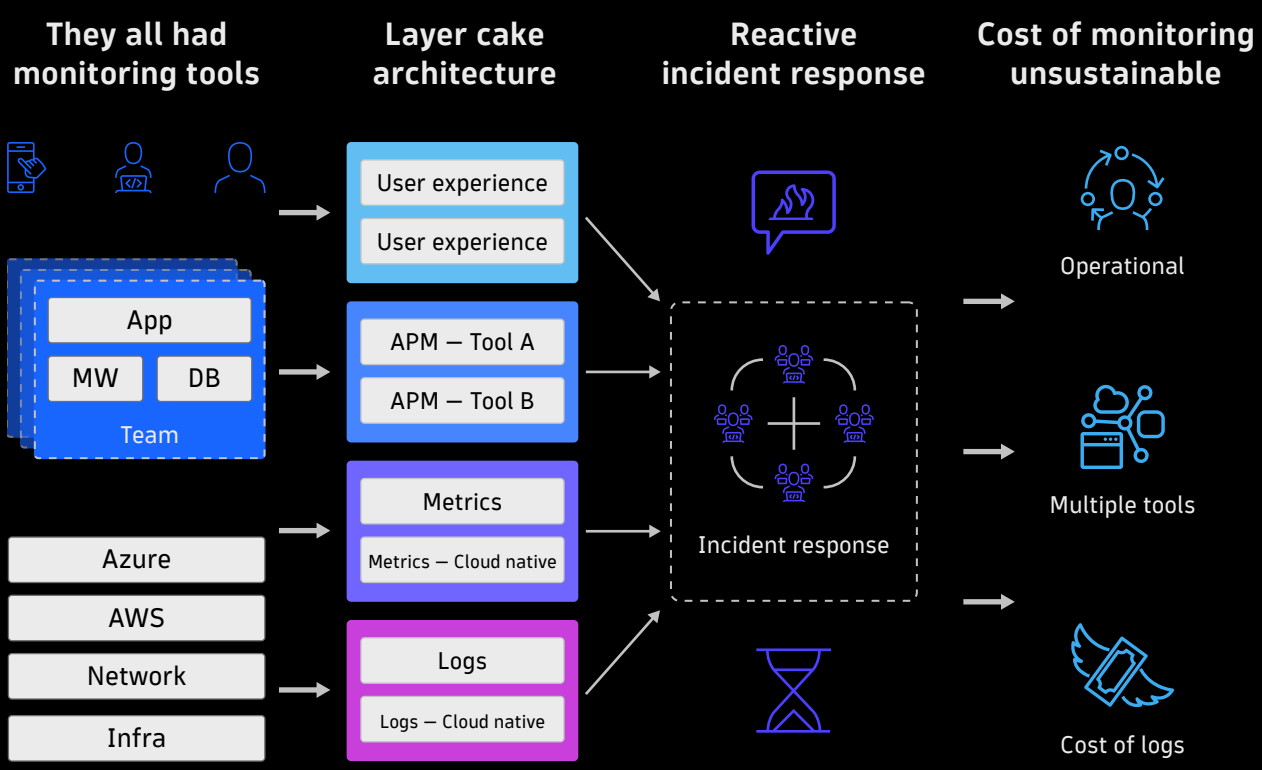


Figure 1: The hidden tax on government IT

The agencies getting on top of this challenge are not doing it by working harder. They are doing it by removing the complexity that made toil necessary in the first place.

SECTION TWO

A different model: Three moves that reinforce each other

Encouragingly, the path forward is not a big-bang transformation. It is three interlocking moves, each of which delivers value independently and compounds when combined.

1. Consolidate visibility

Consolidating tools onto a single unified observability platform cuts licensing costs, but that is the lesser benefit. The bigger gain is something most agencies do not currently have: a single, integrated view of the entire technology stack, from mainframe to multi-cloud, from infrastructure through end-user experience.

When something goes wrong or is about to, the team sees it in one place, in context with what caused it and what it affects, without manually correlating across systems. The positive impact on mean-time-to-resolution is significant, supporting a first-class service delivery experience and a positive impact for the engineers you want to retain.

This is achievable without a rip-and-replace programme. The practical path is consolidation by sunsetting: after adopting the unified platform, as individual tool contracts come up for renewal, do not renew them. Replace the function with what the unified platform already covers. Most organisations find they can retire four to six tools in the first 12 months without a single additional deployment.

2. Reduce the toil driven by answers, not guesses.

The observability problem is not just about visibility. It is about what happens when a problem starts to form or after an incident occurs. Today, that is mostly manual: someone gets paged, logs on to the system, performs swivel-chair correlation, escalates, conferences in three teams, executes a runbook. In an environment where teams are shrinking and telemetry volumes are growing, that sequence doesn't scale.

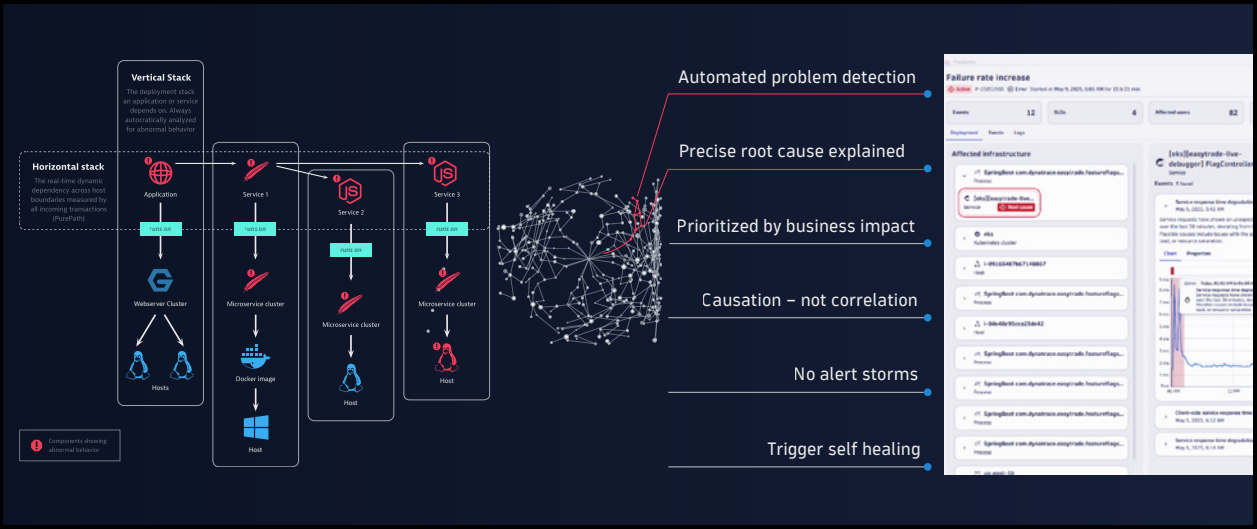


Figure 2: Delivering answers from complexity

The Dynatrace observability platform is powered by Dynatrace Intelligence, a three-tiered AI engine that goes beyond surfacing anomalies. It determines root cause, correlates events across the entire topology in real time, and can orchestrate autonomous responses while your team creates system-level solutions. This is not probabilistic noise reduction. It's precise causal analysis that cuts through alert fatigue and hands your team a solution to implement, not a haystack to search.

For agencies running 24/7 critical services with fewer people, that is not a nice-to-have. It is a sustainability requirement.

3. Enable innovation and AI delivery safely

Almost every agency has AI initiatives in flight or on the roadmap. The pressure to deliver AI-enabled services is growing: faster processing, better citizen self-service, smarter fraud and cyber incident detection. What most agencies have not yet solved is how to establish trust in AI so they can advance their systems from pilot to production and to govern, monitor, and evolve them once they are in production.

Probabilistic AI systems often operate as a black box, and you can't manage what you can't observe. Unified observability of all infrastructure and applications provides a deterministic fact basis for monitoring AI embedded in those applications: model performance, data quality, inference latency, unexpected drift. Agencies that build this capability now are the ones who will be able to safely accelerate AI delivery, with trust and speed.

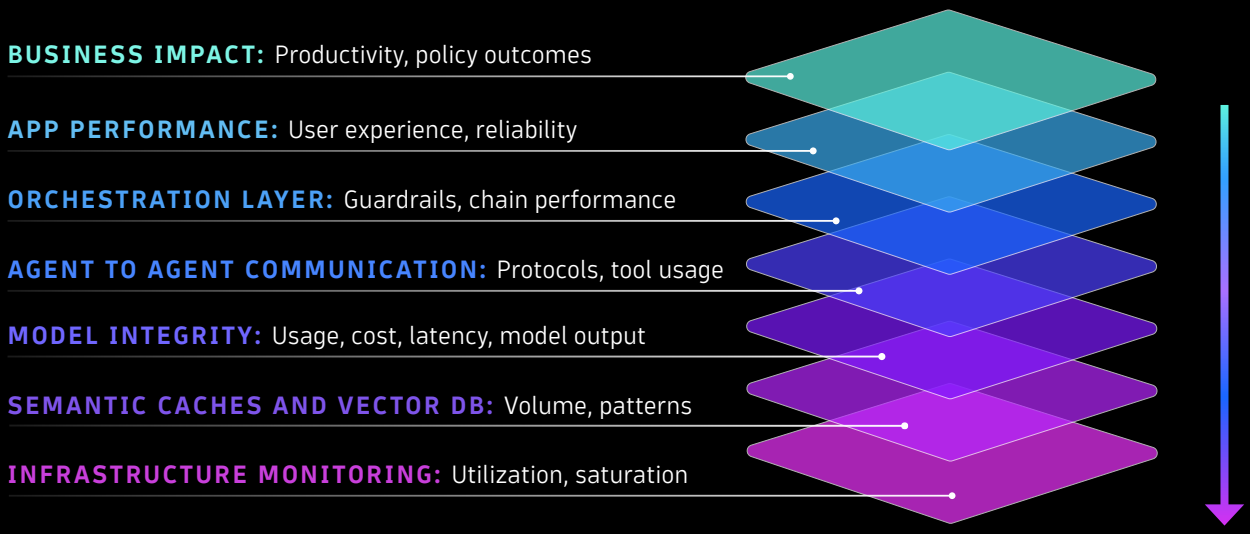


Figure 3: AI Observability in the context of applications

The responsible adoption of AI depends on end-to-end observability. In a climate where the DTA's 2025 Implementation Plan[4] explicitly calls for expanded responsible AI use across government, it is this transparency that your stakeholders and auditors will expect to see in place.

SECTION THREE

Where to start: a realistic 90-day plan

None of the above requires a rip-and-replace before you see value. Here is a practical sequence.

WEEKS 1-2

Know what you have

Run a thorough audit of your current observability and monitoring tooling. How many tools do you have? What do they cover? Where are the overlaps, and where are the gaps?

Most agencies find this exercise clarifying, and often alarming. It also identifies your earliest consolidation candidates and flags the contracts coming up for renewal. Baseline your current mean time to resolution, alert volume, and on-call hours so you have something concrete to measure against.

WEEKS 3-6

Run a targeted pilot

Select one critical workload: a high-traffic citizen service, a core back-office platform, or a security-sensitive system. Deploy Dynatrace to solve it. Full-stack observability starts right away, and actionable insights typically arrive within hours, not weeks.

WEEKS 7-12

Measure, then build the case.

By week 12 you have real data: reduction in alert noise, improvement in resolution time, engineer hours saved per incident. That data is your business case for broader consolidation. Not a vendor presentation, but your own numbers from your own environment.

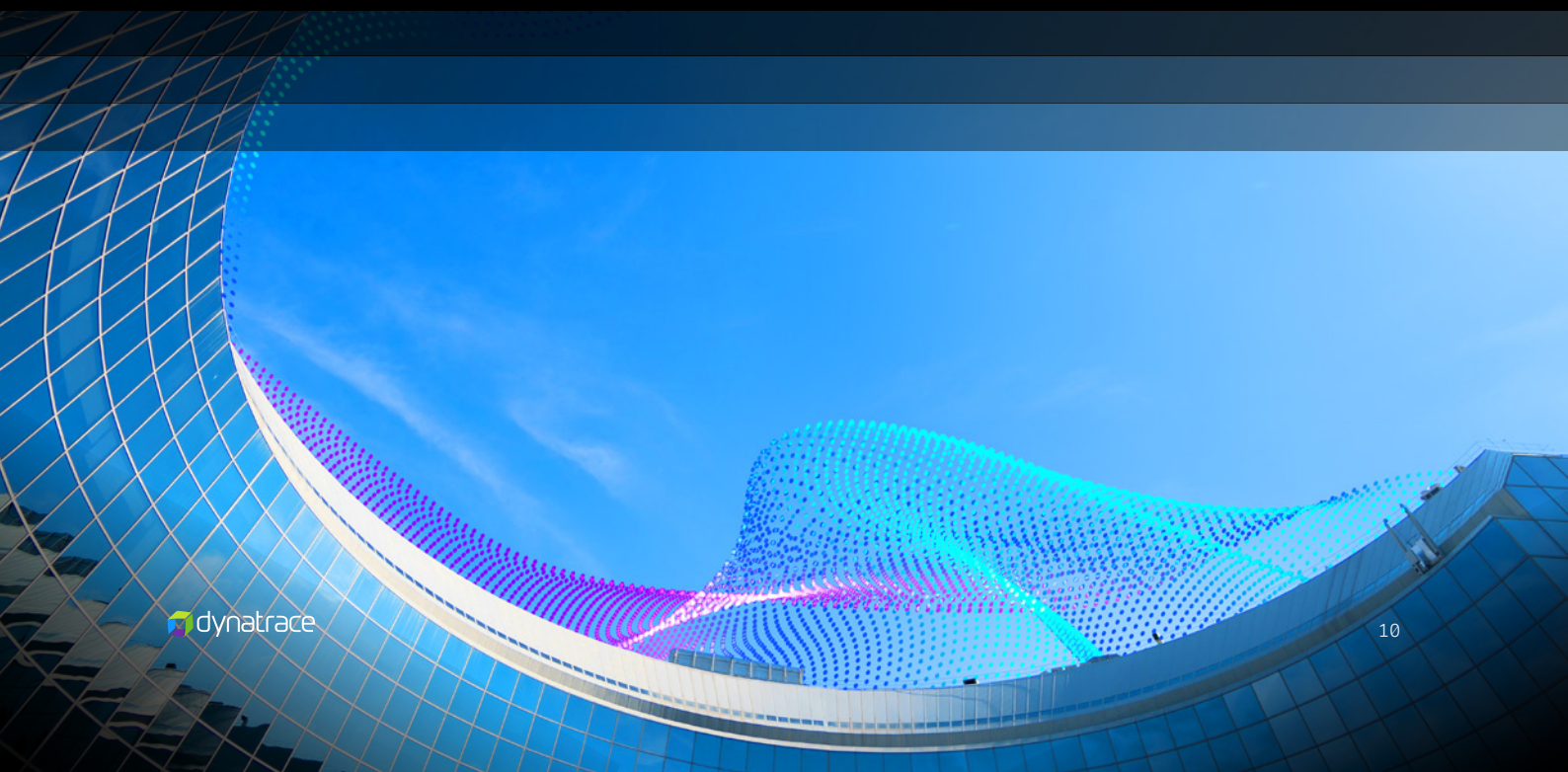
Importantly, Dynatrace SaaS is IRAP-assessed to PROTECTED on both AWS and Azure and provides sensitive data masking capabilities, simplifying the compliance process from day one.

The time-to-value reality

In a budget environment where every dollar needs to justify itself within the current financial year, the pace of adoption matters. The ROI conversation becomes concrete within a single quarter, not a financial year. This is where Dynatrace excels.

Our customers often gain full-stack visibility on a new environment within hours to days, not weeks. Automated root cause analysis is active from day one. Most customers achieve measurable improvement in incident response within 30 days of deployment.

The work of rationalising your full tooling estate takes time, and it should. The value you generate while doing it starts immediately. In the current environment, that is the only kind of transformation you can afford to run.



Doing more with less

Why doing more with less at scale starts with doing one thing with more precision, then expanding

Reach out to our Public Sector team to help you explore where you are and how you can rapidly show value to your organisation.

Dynatrace is IRAP-assessed to PROTECTED on both AWS and Azure, making it deployment-ready for Australian Government environments at PROTECTED classification. To explore what this means for your agency, contact your Dynatrace account team or visit dynatrace.com/au/government.

SOURCES

1. Australian Government Budget 2025-26 efficiency dividend. Agencies directed to identify savings of 5% of annual budgets. Region Canberra, May 2025. region.com.au/federal-budget-not-looking-good-for-the-public-service
2. Dynatrace, The State of Observability in Public Sector Organisations, 2024. Survey of 130 global public sector CIOs and senior IT leaders. dynatrace.com/info/reports/state-of-observability-2024
3. Australian Signals Directorate, Annual Cyber Threat Report 2024-25. cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025
4. Digital Transformation Agency, Data and Digital Government Strategy Implementation Plan 2025. dta.gov.au/media-releases/driving-australias-digital-future-2025-implementation-plan

06.05.26 BAE25726-wp-USLet-cs