guardsix

Playbook

Sovereign security under CADA

Sovereign control is becoming the standard for regulated organisations

On 3 June 2026, the European Commission proposed the Cloud and AI Development Act, part of its Technological Sovereignty Package.

It is designed to address a problem that has been building for years. Europe relies on providers outside the EU for more than 80 per cent of its critical digital infrastructure, and three US firms hold around 70 per cent of the European cloud market. Most regulated organisations no longer control where their security data lives, who operates the systems that hold it, or whose law can reach it.

CADA sets out to change that. It grades cloud and AI services across four sovereignty levels and steers sensitive workloads towards providers that can keep data under European control.

For a regulated mid-market organisations with public sector exposure, this raises the bar. Success is no longer defined by technical capability alone. It is defined by the ability to demonstrate control, produce evidence, and operate consistently under pressure - with the lean team you already have.

It is more than a compliance question. The proposed legislation revolves around operational readiness: can you run your security operations on your own terms, under your own jurisdiction, and prove it? Can you protect the patients, citizens, and communities who depend on you, and show that control never left your jurisdiction?

This playbook explores how regulated organisations can build the operational maturity that sovereignty now demands: meeting CADA and NIS2 together, keeping control where it belongs, and standing behind a sovereignty claim you can defend.

Who CADA applies to

- Cloud and AI service providers and data-centre operators: graded against CADA's four sovereignty levels and required to meet them to qualify for European public-sector contracts.
- EU public-sector bodies: required to assess whether a cloud or AI service is sufficiently protected from foreign control before they buy it.
- Regulated organisations in critical sectors: this includes energy, utilities, healthcare, municipalities, and other organisations exposed to CADA through the public contracts they hold.

The first two carry direct obligations under CADA. The third are subject to CADA because of the data their workflows process: if you serve the public sector or run critical infrastructure, CADA reshapes your tech stack and defines the sovereignty level your workloads must meet.

A changed compliance conversation

For years, cyber security conversations focused on prevention, detection, and response. Buying new technologies, adding controls, and growing the stack was the primary way security leaders reduced risk.

CADA changes that. The question is no longer only what you buy or how well it detects. It is where your security data lives, who operates the systems that hold it, and whose law governs them. NIS2 asked you to prove control. CADA asks you to prove it is sovereign control.

When a regulator, an auditor, or your own board asks, they are not interested in product specifications. They want answers.

- Where does your security data live?
- Who operates the systems that hold it?
- Whose law can reach it?
- What evidence supports the decisions you made, and can you produce it on demand?
- Does that control still hold if a vendor, or another country, changes the terms?

These questions sit at the heart of CADA. They show where cloud dependency risk gets expressed in real-world context. A reassuring data-centre location tells you nothing about who can reach the data, or who can change the terms. Where and how you operate becomes just as important as how well you detect.

The organisations best positioned to succeed are not the ones with the largest technology budgets. They are the ones that can demonstrate sovereign control, consistency, and preparedness.

The accountability challenge

Running security for a regulated organisation carries a complexity that regulation rarely acknowledges. CADA adds a sharper edge: you now must hold sovereign control across every system you run, not just consistent practice.

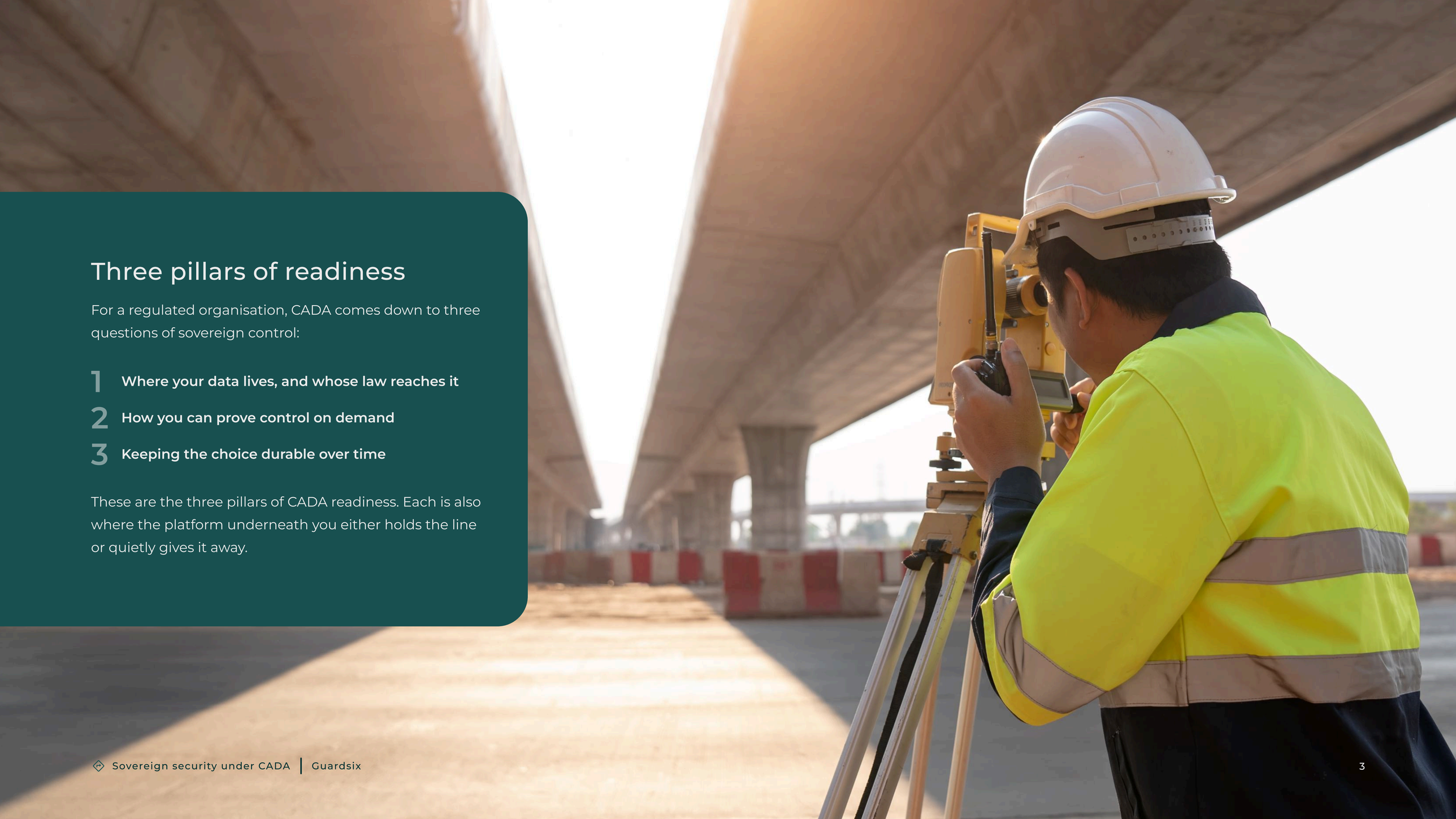
Healthcare, energy, and municipalities each carry their own pressure. A health provider answers to GDPR Article 32 and national patient-data rules. A utility sits squarely in scope for NIS2 as an essential entity. A municipality has to keep citizen data in citizen jurisdiction and defend every choice through public procurement.

Most teams meet this with thin headcount. Lean security teams of fewer than ten people, often only two or three in a municipality, carry the full weight of monitoring, investigation, reporting, and evidence. The issue is rarely a lack of technical capability. It is holding visibility, documentation, and sovereign control across fragmented systems, and being able to prove it.

At the same time, the stakes have risen. Under NIS2, fines for essential entities reach up to €10 million or 2 per cent of global turnover, and Article 20 makes management personally accountable for cyber security risk measures — with temporary management bans on the table for repeated failures.

An organisation may have detected and even responded to an incident well. But if the investigation cannot be reconstructed, if decisions are undocumented, or if you cannot show where the data sat and who could reach it, confidence disappears quickly.

CADA places greater emphasis on proving sovereign control. That requires structure.



Three pillars of readiness

For a regulated organisation, CADA comes down to three questions of sovereign control:

1. **Where your data lives, and whose law reaches it**
2. **How you can prove control on demand**
3. **Keeping the choice durable over time**

These are the three pillars of CADA readiness. Each is also where the platform underneath you either holds the line or quietly gives it away.

1 Where your data lives, and whose law reaches it

Sovereign control starts with a physical fact: where your security data sits, and whose law can compel access to it.

NIS2 already made leadership accountable for this. Under Article 20, management bodies must approve cyber security risk measures, oversee their implementation and can be held personally liable for failing to do so.

CADA adds the sovereignty question on top. It is no longer enough to know your controls work. You must know where the data sits and whose jurisdiction governs it.

This is the question cloud-first platforms struggle to answer. If your security data is processed on infrastructure operated by a foreign provider, it can sit within reach of foreign law, the US CLOUD Act and FISA among them, no matter where the data centre is.

The point is not theoretical: in 2025, Microsoft's own French legal director conceded under oath that the company could not guarantee French citizens' data would never be passed to US authorities. A reassuring contract clause, or a "sovereign cloud" label, is not the same as a jurisdiction you control.

2 How you can prove control on demand

NIS2 requires organisations to put appropriate and proportionate measures in place to manage cyber security risk. CADA extends the same logic to sovereignty.

It sets out four levels of cloud and AI sovereignty and steers sensitive workloads towards providers that can show European control and independence from foreign law.

The question is no longer only whether your controls work. It is whether you can show, at the level the workload demands, that control sits in trusted hands.

When the evidence lives in systems you run — a continuous account of who accessed what data, when, under what authorisation, and within which jurisdiction — you can produce it the day the auditor walks in. When it sits in a vendor-operated cloud, you are waiting on someone else to hand you your own proof.

3 Keeping the choice durable over time

A sovereign choice is only sovereign if you can afford to keep it. You need to know whether the control you need today is still yours at the next renewal, the next traffic spike, and the next budget round.

Two convenient answers tend to fail under this pressure. The first is a “sovereign cloud” — a familiar provider wrapped in a reassuring label. But the label is the easy part. If the infrastructure is still operated by a foreign provider, the data still sits within reach of foreign law, whatever the contract says. A sovereign cloud can look like control while quietly keeping it somewhere else.

The second is open-source tooling you host yourself. Free licensing is a powerful draw, and a self-built stack can be genuinely sovereign. But for a lean security team, the cost quickly becomes uneconomical: building, tuning, and maintaining the stack requires headcount the team does not have.

Durability means pricing you can plan around and a roadmap that keeps backing the choice you made. Sovereign, on-prem deployments provided by EU-headquartered vendors offer clear advantages to the lean teams that Europe’s regulated mid-market organisations rely on.

What CADA asks of you

One thing to keep in mind: CADA is still a proposal. It needs agreement from all 27 member states and the European Parliament, with trilogue negotiations expected through 2026 and adoption unlikely before 2027. But the direction is not in doubt, and it lands on the same points NIS2 has already made.

You must be able to show where your data lives, who can reach it, and that control sits in trusted hands. For a regulated organisation, that is more than a compliance task: it changes the risk calculus your board, your regulator, and your procurement team apply to every decision.

The same discipline that satisfies CADA is what lets you stand behind a sovereignty claim in front of the people you serve.

The hidden challenge: proving sovereign control

One of the least discussed aspects of sovereignty is evidence. Most teams focus on security operations; far fewer focus on proving what happened afterwards.

When a regulator, a public citizen, or your own board asks questions, evidence becomes essential.
It demonstrates that:

- risks were understood
- controls were operating
- decisions were reasonable
- incidents were managed appropriately
- data stayed where it was meant to, reachable only by those it was meant for

Without evidence, you are left to rely on assumptions and memory. The real exposure is not whether that approach scales. It is what it puts at risk: a failed audit, a missed reporting deadline, a sovereignty claim you cannot back up, and the heavier scrutiny that follows.

The ability to produce defensible evidence quickly, from systems you operate, is becoming a defining characteristic of mature security operations.

What mature regulated teams do differently

The most effective teams do not necessarily have more tools. They:

- hold sovereign control of their own data and tooling
- run repeatable processes
- follow a structured approach to investigations
- produce standardised reporting
- work from a common set of workflows

Operational maturity is reached when outcomes stay consistent, and control stays in your hands, regardless of which analyst is handling an investigation or which system is affected.

That consistency matters most under the pressure each sector already feels. Ransomware accounts for more than half of all cyber threats to the health sector, according to ENISA, and is increasingly prevalent against municipalities across the EU.

When an incident hits a hospital, a utility, or a town hall, the question that follows is always the same: can you show what happened, and that the data never left your control? Consistency is what lets you answer.

Where Guardsix fits

Guardsix helps regulated organisations hold sovereign control across every system they run: audit-ready log management, centralised visibility, and evidence you operate yourself rather than rent from a vendor.

Our platform helps lean security teams investigate incidents efficiently, demonstrate control confidently, and support reporting obligations without adding complexity. In practice, that rests on three things.

1. **European jurisdiction**
   Guardsix is EU-headquartered and governed by European law alone, so your security data, audit trails, and access logs sit under one jurisdiction — the one you can answer for.
2. **Predictable pricing**
   Node-based pricing scales with the infrastructure you run, not the data you generate. No ingestion surprises, no year-two reset.
3. **An active on-prem roadmap**
   Staying off the cloud is a direction we keep investing in, not a legacy option we are quietly winding down.

That combination produces the outcomes regulated teams buy today: sovereign log management that keeps every log on European soil, audit-ready evidence that maps straight to compliance controls, and patient-record access governance for healthcare providers to prove who accessed which record, when and why, in one defensible place.

As CADA moves Europe towards graded sovereignty, European infrastructure stops being a preference and becomes the basis on which you keep the trust of the people you serve.

When they rely on you this closely, you need more than a vendor. You need a close ally.

Sources: cloud market concentration and non-EU digital reliance — Synergy Research Group (2025) and the Draghi report, as cited in the EU's Tech Sovereignty Package communication; CADA provisions, scope, and four-level sovereignty framework, including public-sector procurement criteria for assessing protection from foreign control — European Commission, Cloud and AI Development Act (proposed 3 June 2026); NIS2 penalties and management liability — Directive (EU) 2022/2555, Articles 20 and 34; Microsoft testimony — reported May 2026; health-sector and municipal ransomware figures — ENISA Threat Landscape reporting.

Conclusion

CADA comes in the form of a compliance regime, but in practice it is something more fundamental: a test of sovereign control, building on the operational readiness NIS2 already asks of you.

For a regulated organisation, success will not be determined by the size of the technology stack or the number of tools deployed. It will be determined by the ability to remain in sovereign control when expectations are highest.

The patients, citizens, and communities you serve rely on you for answers, evidence, and confidence when it matters most. When that much depends on you, you deserve a partner who has your six.

Found this playbook useful?

Learn more | Get in contact

guardsix

Guardsix (formerly Logpoint) is a European cybersecurity company headquartered in Copenhagen, Denmark, providing a sovereign security platform for MSSPs and regulated organisations. Its unified platform combines SIEM, NDR and SOAR and fleet management capabilities to help organisations achieve audit readiness, detect advanced threats and scale security operations with confidence.