



Beyond Compliance

Aruba's Strategic Control Stack for navigating
eIDAS 2.0, NIS2, DORA, and the AI Act.

aruba.it

puise

Summary

01 Europe's control imperative	4
02 What organisations are really struggling with	6
03 Four answers to one control problem	7
04 Aruba's distinctive position: CSP+QTSP across Europe	10
05 eIDAS 2.0: trusted identity as infrastructure	14
06 NIS2: cybersecurity as structural baseline	16
07 DORA: operational resilience as design principle	18
08 AI Act: governance as infrastructure prerequisite	20
09 The buying framework	23
10 Beyond compliance, toward control	26

PART I

The Control Architecture

CHAPTER 01

Europe's control imperative

Europe's digital economy is entering a new phase. For years, progress was measured mainly by speed, scale, and efficiency. Today, that is no longer enough. As organisations operate across cloud environments, external providers, digital identity systems, and AI-enabled workflows, the central challenge is no longer just digitisation. It is maintaining control: ensuring that systems remain trustworthy, resilient, and governable over time.

The real issue is not whether to adopt more technology. It is who governs the digital foundations.

This is why eIDAS 2.0, NIS2, DORA, and the AI Act matter. They are not isolated rules. They are part of a broader European effort to ensure that digital systems can be trusted, essential services remain operational, cyber risks are controlled, and AI is deployed responsibly.

Regulation is structural, not optional. The real question is not how fast organisations innovate, but whether they remain in control of the systems that enable that innovation.

The common thread across these measures is not compliance for its own sake. It is control. Each regulation addresses a different layer of the same problem, but all push organisations toward the same conclusion.

Compliance should be embedded from the start, not bolted on afterwards as a tool.

eIDAS 2.0 is about trusted identity. DORA is about operational resilience in finance. The AI Act is about governing artificial intelligence. NIS2 is about baseline cybersecurity. Together, they form a coherent framework for building digital systems that are trusted, resilient, and accountable.

Together, they are also changing how organisations buy. Compliance is increasingly becoming a selection criterion in European procurement, particularly where identity, resilience, auditability, and sovereign infrastructure must be demonstrated together. For procurement teams, this is no longer a back-office consideration. It is the design of the buying decision itself.



CHAPTER 02

What organisations are really struggling with

Most organisations did not design their digital environments as a coherent system. Infrastructure, identity, cybersecurity, and trust mechanisms evolved separately, often across multiple vendors and geographies. The result is a loss of visibility and control.

The six structural pressures

- **Fragmented digital infrastructure:** layers selected independently, not designed for resilience or auditability.
- **Growing third-party dependence:** concentration risk, supply chain exposure, vendor compliance burden.
- **Identity sprawl:** fragmented models for users, systems, APIs, and AI agents.
- **Traceability gaps:** difficulty proving who acted, what, when, and under what conditions across ecosystems.

- **Board-level accountability:** risk now demands architectural evidence, not policy assurances.
- **AI governance lag:** amplifies risk without trusted foundations underneath.

Critical processes now depend on systems that organisations do not fully own, do not fully govern, and often cannot fully audit. As a result, demonstrating accountability becomes increasingly difficult, especially across hybrid environments, third-party dependencies, and automated workflows. This leads to a fundamental challenge: **how do organisations maintain control in systems they no longer fully control?**

Regulators, customers, and boards are no longer satisfied with systems that simply function. They require organisations to demonstrate who acted, under what authority, on which infrastructure, and with what safeguards in place. Regaining that level of control, the ability to operate, adapt, and evolve without dependency, is becoming a strategic necessity.

At Aruba, we call this Strategic Control: the ability to govern, adapt, and evolve the entire digital stack while maintaining control and autonomy over infrastructure, data, and decision-making.

This is not achieved through additional tools or policies. It requires architecture: systems designed to embed trust, resilience, traceability, and accountability by design.

CHAPTER 03

Four answers to one control problem

Taken together, eIDAS 2.0, NIS2, DORA, and the AI Act can be understood as four coordinated responses to the same underlying challenge: ensuring that digital systems remain controllable as they become more complex, distributed, and automated.

In this environment, **digital identity is no longer just an access mechanism. It is infrastructure for trust**, enabling organisations to prove who acted, with what authority, and with what legal and operational assurance. It is also the connective layer that makes processes interoperable — allowing identity, signatures, and attestations to be recognised and acted upon across organisations, sectors, and borders without re-integration at each step.

Each measure addresses a different layer, but all push organisations in the same direction: **stronger identity, clearer accountability, greater resilience, and more verifiable operations.**

THE FOUR, ONE BY ONE

1 eIDAS 2.0

Establishes the rules for electronic identification and trust services, enabling organisations to verify identity and validate digital transactions across borders.

In practical terms: **it ensures you can prove who is acting and whether a digital interaction can be trusted.**

3 AI ACT

Introduces a risk-based framework for Artificial Intelligence, imposing stronger obligations as risk increases. In practical terms: **it ensures AI systems are transparent, accountable, and safe to use.**

2 DORA

Defines how financial organisations must ensure continuity under stress, requiring them to prevent, withstand, and recover from ICT disruptions. In practical terms: **it ensures critical services continue to operate even when systems fail or are attacked.**

4 NIS2

Raises the cybersecurity baseline across essential and important sectors. In practical terms: **it ensures organisations systematically manage cyber risk and can demonstrate it.**

HOW THEY FIT TOGETHER

These measures are best understood as parts of a single architecture:

- **eIDAS 2.0** establishes trusted identity and the interoperability of trusted processes;
- **NIS2** secures the environment;
- **DORA** ensures operational continuity;
- the **AI Act** governs the intelligent systems built on top.

They overlap because modern digital services depend on all of them simultaneously.

Trust and security are no longer features to add, but structural elements that enable organisations to operate and evolve without losing control.

WHY THEY WERE BUILT

Europe's objective is not only digital growth, but **controlled digital growth**, where innovation does not come at the cost of dependency, fragility, or loss of oversight.

There is now a supply-side counterpart to this regulatory architecture. Where eIDAS 2.0, NIS2, DORA, and the AI Act set the rules organisations must meet, the proposed Cloud and AI Development Act (CADA) addresses a prior question: whether Europe has the infrastructure to meet them at all. The four regulations create demand for trustworthy, controllable, European-operated compute. CADA is Europe's effort to build the supply.

Regulation sets the rules. CADA builds the capacity. Strategic Control is what connects the two. Sovereignty is architectural, not contractual. It is not about speed. It is about control.

The AI Act moves AI from experimentation into governance. Organisations must now demonstrate how AI systems are designed, trained, deployed, and monitored, including how decisions are made and how risks are managed.

AI cannot be governed if the underlying infrastructure, identity, and control layers are not already trustworthy. Without these foundations, AI does not reduce complexity. It amplifies it.



CHAPTER 04

Aruba's distinctive position: CSP+QTSP across Europe

The challenge for organisations is not ticking four regulatory boxes. It is building a system that restores control, across identity, cybersecurity, operations, and AI, within a coherent European framework. This is what Aruba enables. And the way Aruba enables it is structurally distinctive.

THE INTEGRATED EUROPEAN STACK

Aruba is the only European operator combining **Cloud Service Provider (CSP)** capability and **Qualified Trust Service Provider (QTSP)** capability under a single accountable European operating model. To this combination, Aruba adds proprietary data centre infrastructure, integrated cybersecurity operations, digital identity services, and connectivity, all within a single European jurisdiction.

This combination matters because it answers the four regulations in one architecture rather than four:

- **as a CSP**, Aruba provides european sovereign cloud and proprietary data centre capabilities that address infrastructure, hosting, and operational resilience requirements under NIS2 and DORA;
- **as a QTSP**, Aruba operates qualified trust services through two qualified providers, Actalis (Italy's first Certification Authority) and ArubaPEC, covering digital signatures, certified electronic mail (PEC), timestamping, qualified e-delivery, and digital identity. At continental scale, Aruba's trust services account for over 1.6 billion electronic signatures annually, 9 million PEC mailboxes, over 2 million digital identities issued (SPID), and 2.7 million domains under management;
- **as an integrated operator**, Aruba runs cybersecurity operations from its own SOC, manages a managed detection and response capability, and aligns its security posture to recognised frameworks including NIST CSF;
- **as a European builder and maker**, Aruba designs, builds, and operates its own infrastructure and software rather than reselling capacity from others. This is what makes the trust verifiable: the architecture is not assembled, it is owned.

This is also the posture European industrial policy is now actively encouraging.

The direction of the proposed Cloud and AI Development Act, expanding European-operated compute capacity for sensitive and critical workloads, describes what Aruba already is: an operator that builds and runs its own infrastructure rather than reselling someone else's.

Aruba does not need to become what CADA envisions. It already operates there.

No direct competitor in the European sovereign cloud market matches this combination.

Sovereign cloud peers do not offer qualified trust services. Identity and trust providers do not offer European sovereign cloud or proprietary data centres.

This unique combination remains unmatched within the European market.

The convergence of these four regulations creates a common governance imperative. Strategic Control is designed to address it.

WHAT THIS DELIVERS

Infrastructure is no longer a commodity. It is a strategic asset: the foundation on which control, resilience, and long-term evolution depend.

Aruba approaches this as an architectural problem, not a product one.

By combining European infrastructure, qualified trust services, cybersecurity operations, digital identity, and connectivity within a single European jurisdiction, Aruba provides a unified operating model where control is built in, not reconstructed afterwards.

This allows organisations to:

- **maintain** full visibility across their digital environments;
- **reduce** dependency on fragmented providers;
- **demonstrate** compliance as a natural outcome of architecture;
- **evolve** continuously without losing control.

THE PROGRESSIVE MODEL

Aruba delivers this through four progressive stages:

- **Enable** - European-native foundations and ready to use solutions across infrastructure, cloud, connectivity, trust, and security;
- **Enhance** - Managed and orchestrated services that bring together multiple capabilities into coherent solutions, reducing fragmentation and creating a single point of accountability;
- **Empower** - Co-design of tailored solutions that bring together the right mix of infrastructure, cloud, cybersecurity, trust, AI, and managed services to support strategic objectives;
- **Evolve** - Active participation in European ecosystems, shaping interoperability standards and future trust frameworks.

This goes beyond compliance support. It is the restoration of organisational control over digital infrastructure.

PART II

Regulation by Regulation

CHAPTER 05

eIDAS 2.0: trusted identity as infrastructure

The structural question

Can your organisation prove, at scale and across borders, who is acting in a digital transaction and whether that action is legally binding?

eIDAS 2.0 is the European framework for electronic identification and qualified trust services. Its reform, culminating in the European Digital Identity Wallet, moves identity from a credential held by the user to an interoperable infrastructure operated across the Single Market.

Architectural implications

The shift from eIDAS 1.0 to 2.0 reframes identity in four ways. First, identity becomes wallet-centric: citizens and businesses control credentials they present to public and private services. Second, identity becomes interoperable: the same wallet works across Member States, sectors, and use cases. Third, identity becomes attribute-rich: beyond authentication, the

wallet carries qualified electronic attestations of attributes (QEAA) and verified business information. Fourth, identity becomes operational at scale: from KYC and onboarding to contract execution, identity is no longer an entry point but a continuous trust layer.

For organisations, this translates into specific architectural requirements:

- the capability to issue, present, and verify wallet-based identity credentials;
- the capability to integrate with qualified trust services for electronic signatures, seals, timestamps, and e-delivery;
- the capability to manage cross-border identity flows without re-integration in each jurisdiction;
- the capability to validate identity continuously, not only at first access.

Intersections

eIDAS 2.0 is the identity layer that makes the other three regulations operable. Under DORA, identity is how financial operators prove who initiated which action under stress. Under NIS2, identity governance is one of the core cybersecurity baseline requirements. Under the AI Act, identity is how organisations distinguish human action from automated action, and how they audit AI-mediated decisions.

What Aruba delivers

Through its qualified trust providers, Actalis (Italy's first Certification Authority and a founding QTSP in Europe) and ArubaPEC, Aruba operates qualified trust services at continental scale: digital signatures, PEC certified email, timestamping, qualified e-delivery (QeRDS), digital identity (including SPID), identity verification, and electronic attestations. Aruba's Wallet Gateway provides the integration layer through which organisations consume EUDI Wallet capabilities without rebuilding identity infrastructure per country or per use case. Aruba leads in the POTENTIAL and WeBuild LSP (Large Scale Pilot) projects under the European Digital Identity Framework, where it operates at the intersection of qualified trust services, wallet integration, and cross-border operability.

See **Aruba's Wallet paper** for the operational toolkit on EUDI Wallet integration, QES/QEAA/QeRDS, and cross-border identity flows.

CHAPTER 06

NIS2: cybersecurity as structural baseline

The structural question

Can your organisation demonstrate, with evidence, that cybersecurity is governed as a structural capability rather than as a layer of tools and policies?

NIS2 raises the cybersecurity baseline across essential and important sectors, formalising what was previously good practice into legal obligation. It moves cybersecurity from an IT function reporting upward to a board-level accountability requiring architectural evidence.

Architectural implications

NIS2 translates into specific architectural requirements that reach beyond traditional security controls:

- risk management measures must be commensurate with the entity's size, sector, and exposure and demonstrable;
- incident reporting must be timely, structured, and consistent across the supply chain;
- supply chain security must be governed, not assumed, including ICT third parties;
- governance bodies (boards, management) bear personal accountability for cybersecurity posture;
- security testing, training, and continuous improvement must be evidenced, not declared;
- key cybersecurity capabilities, SOC, vulnerability management, incident response, business continuity, must be either operated in-house at appropriate maturity or sourced from qualified providers.

Intersections

NIS2 is the security baseline on which DORA's resilience requirements build, the identity governance layer that eIDAS 2.0 makes operational, and the trust foundation that the AI Act presumes when it requires AI systems to operate on secure infrastructure. NIS2 is the regulation that, if absent, undermines all three of the others.

What Aruba delivers

Aruba operates its own Security Operations Centre on a 24x7 basis, with managed detection and response (MDR) and extended detection and response (xMDR) capabilities.

Aruba's security posture is aligned to the NIST Cybersecurity Framework, with regular vulnerability assessment and penetration testing (VAPT), web application protection (WAP), and dedicated anti-DDoS infrastructure.

Aruba is its own first and largest cybersecurity client: the same operational maturity that safeguards Aruba's digital ecosystem and customer base is the maturity that Aruba offers as a service.

For organisations seeking to meet NIS2 obligations through a qualified European provider, Aruba offers two operating models: managed (SaaS) cybersecurity for those who need integrated capability, and self-managed (PaaS) cybersecurity for those who retain in-house operations but need European-jurisdiction infrastructure beneath them.

See **Aruba's Cybersecurity paper** for the structural model, managed vs self-managed, the NIST CSF alignment, and the integration with trust services.

CHAPTER 07

DORA: operational resilience as design principle

The structural question

Can your organisation continue to deliver critical services when third-party ICT systems fail, are attacked, or become unavailable?

DORA, the Digital Operational Resilience Act, applies to financial entities and the ICT third-party providers that serve them. It moves resilience from a contingency-plan exercise to a continuous, evidenced operational discipline, covering ICT risk management, incident reporting, digital operational resilience testing, third-party risk management, and information sharing.

Architectural implications

DORA translates resilience into architecture in five domains:

- **ICT risk management** - governance frameworks, asset inventories, classification of critical functions;
- **ICT-related incident management** - detection, reporting, response, and root cause analysis under tight timelines;
- **Digital operational resilience testing** - from vulnerability assessment to threat-led penetration testing (TLPT) for significant entities;
- **ICT third-party risk management** - contractual clauses, register of information, concentration risk monitoring, exit strategies;
- **Information sharing arrangements** - cross-organisation intelligence flow on threats and vulnerabilities.

The most consequential of these for buyers is the third-party risk dimension.

DORA forces financial entities to ask their ICT providers questions that previously were not asked of cloud, hosting, or SaaS vendors at all, about sub-outsourcing, geographic location of data and operations, audit rights, exit feasibility, and concentration risk.

Intersections

DORA is the resilience operationalisation of what NIS2 sets as a baseline, applied with sectoral precision to finance. It depends on eIDAS 2.0 for identity verification under stress conditions, and it overlaps with the AI Act where financial entities deploy AI in customer-facing or risk-decision functions.

What Aruba delivers

Aruba's positioning under DORA is direct: as a European-jurisdiction ICT provider with proprietary infrastructure, qualified trust services, and integrated cybersecurity, Aruba reduces both the contractual surface area and the operational risk profile that DORA scrutinises.

Aruba's contracts can satisfy DORA's required clauses on sub-outsourcing limits, audit rights, exit strategies, and geographical operating boundaries. Aruba's operational profile, proprietary data centres, redundant connectivity, certified resilience, addresses the substance of what those clauses ask for. For financial entities navigating DORA, the question is not only whether a provider can sign the right clauses, but whether the provider's architecture can deliver what the clauses describe. Aruba's architecture is built to deliver both.

See **Aruba's DORA Pulse paper** for the operational toolkit: contractual clauses, register of information requirements, third-party risk mapping, testing roadmap, and the six-point Aruba positioning.



CHAPTER 08

AI Act: governance as infrastructure prerequisite

The structural question

Can your organisation deploy AI systems whose decisions, training data, and operating environment are auditable end-to-end?

The AI Act introduces a risk-based framework for Artificial Intelligence systems, with obligations rising with risk classification. Prohibited practices are banned. High-risk systems face documentation, testing, monitoring, transparency, and human oversight obligations.

General-purpose AI models face specific obligations on transparency, copyright, and systemic risk. Limited-risk systems face disclosure obligations.

Architectural implications

The AI Act's most important architectural implication is not what it says about AI, it is what it presumes about the layers underneath AI. To meet AI Act obligations, an organisation must already have:

- trustworthy infrastructure to run AI workloads with documented provenance;
- qualified identity to distinguish human action from automated action and to authenticate users of high-risk AI systems;
- cybersecurity baseline to protect AI training data, model weights, and inference pipelines;
- operational resilience to ensure AI-mediated services degrade gracefully;
- traceability across the AI lifecycle: data sources, training runs, deployment changes, monitoring logs.

In other words, the AI Act presumes the work that eIDAS 2.0, NIS2, and DORA require. Organisations that have not built those foundations will find AI Act compliance far more difficult than the AI Act itself suggests, because the AI Act treats those foundations as given.

Intersections

The AI Act sits on top of the other three. Identity (eIDAS 2.0), security (NIS2), and resilience (DORA) are not parallel obligations, they are prerequisites. An organisation that addresses the AI Act in isolation from the other three will end up rebuilding the foundations as it goes.

What Aruba delivers

Aruba's AI proposition is deliberately not a model proposition. Aruba does not offer proprietary LLMs. Aruba offers the European foundations on which AI can be deployed responsibly: European infrastructure for compute (CPU and GPU), private AI platform options for regulated industries, multi-model orchestration without proprietary lock-in, qualified trust services that authenticate AI-mediated transactions, cybersecurity operations that protect training data and inference pipelines, and energy from proprietary hydroelectric sources that addresses sustainability questions in AI Act risk assessments.

For organisations seeking to deploy AI under the AI Act, the question is not which model to choose, it is whether the foundations beneath the model can be evidenced. Aruba's role is to make those foundations evidenceable.

A note on CADA. The AI Act governs how AI may be used; the proposed Cloud and AI Development Act addresses whether Europe has the compute to run it. The two are complementary, one sets the obligations, the other builds the capacity to discharge them on European-operated infrastructure.

For organisations deploying AI under the AI Act, CADA signals that European-jurisdiction compute for sensitive and high-risk workloads is not a niche preference but an explicit policy priority. That strengthens, rather than complicates, the case for building AI on foundations that are European by design.

PART III

From Regulation to Architecture



CHAPTER 09

The buying framework

The four regulations translate into specific control requirements, which translate into architectural answers, which translate into provider capabilities. The matrix below is designed to be used in the order in which procurement teams actually work: **regulation → control requirement → architectural answer → Aruba capability**.

It is not exhaustive. It is the structural shortlist of what a buying committee should be able to evidence and what a provider should be able to demonstrate.

For full operational depth on any row, the relevant Aruba dedicated paper provides the toolkit.

REGULATION	KEY CONTROL REQUIREMENT	ARCHITECTURAL ANSWER	ARUBA CAPABILITY
eIDAS 2.0	Cross-border identity verification at scale	Wallet-integrated qualified verification operating across Member States	Aruba Wallet Gateway + Actalis QTSP + POTENTIAL/WeBuild LSP participation
eIDAS 2.0	Qualified electronic signature, seal, and timestamp	Continuous QTSP operation under single EU jurisdiction	Actalis + ArubaPEC (qualified trust providers): 1.6B annual signatures, full QES/QESeal/QTS/QeRDS
eIDAS 2.0	Trusted e-delivery and legal-value notification	PEC and QeRDS infrastructure operated end-to-end in Europe	Aruba PEC (10M mailboxes) + Aruba Sign + qualified e-delivery
NIS2	24x7 SOC operations and incident response	Operated SOC with managed and extended detection and response	Aruba SOC + MDR/xMDR services + NIST CSF alignment
NIS2	Supply chain security and ICT third-party governance	European-jurisdiction provider with proprietary infrastructure	Aruba as builder & maker: no sub-outsourcing of core capabilities
NIS2	Vulnerability management and security testing	VAPT, web application protection, anti -DDoS as continuous services	Aruba VAPT + Web Application Protection + dedicated anti-DDoS infrastructure
NIS2	Board-level evidence of cybersecurity posture	Documented architecture, certifications, and audit trails	ISO 27001 + Tier IV DCs + ACN QC3 + NIST CSF alignment + audit -grade logging
DORA	ICT third-party contractual clauses (sub-outsourcing, audit, exit)	Provider whose architecture matches what the clauses describe	Aruba DORA-aligned contracts + proprietary infrastructure under EU jurisdiction
DORA	Register of information requirements	Provider able to deliver structured information on locations and sub-providers	Aruba Information Pack for DORA + transparent geographic operating model
DORA	Concentration risk and exit feasibility	Alternative European provider with full-stack capability	Aruba as primary or secondary European provider + Multi-Cloud Link for hybrid models
DORA	Threat-led penetration testing (TLPT) participation	Provider capable of engaging in TLPT scenarios with financial entities	Aruba SOC + dedicated security engagement model for financial sector
AI ACT	European infrastructure for AI workloads	EU-jurisdiction compute (CPU and GPU) with documented provenance	Aruba AI Platform + AI Endpoints + sovereign GPU + Private AI Platform
AI ACT	Trusted authentication of AI-mediated actions	Qualified identity layer integrated with AI workflows	Actalis QTSP + Wallet Gateway + identity infrastructure for AI agents
AI ACT	AI lifecycle traceability and audit	Infrastructure logging and traceability across the full AI stack	Aruba Cloud + AI Platform with audit -grade logging + multi-model orchestration

The matrix is not a checklist.

It is a structural map: each row shows how a regulatory requirement translates into an architectural choice, and each architectural choice into a capability that can be evidenced.

The same map reveals something the four regulations do not show in isolation, that the strongest capabilities discharge obligations across multiple regulations at once. A single SOC operation answers to NIS2, DORA, and the AI Act simultaneously. A single qualified trust service answers to eIDAS 2.0 and the AI Act. The architecture compresses what looks like four separate compliance burdens into a coherent operating model.

This is the practical meaning of Strategic Control: not the absence of regulation, but the architecture that makes regulation operable as a single design problem rather than four.



CHAPTER 10

Beyond Compliance, toward Control

Europe stands at a crossroads. Participate in global digital ecosystems while remaining fully in control and EU-compliant, or risk exclusion from both.

eIDAS 2.0, NIS2, DORA, and the AI Act each address different aspects of trust: identity, security, resilience, and AI governance. But together they establish a clear principle:

Digital systems must be secure, resilient, accountable, and controllable by design.

Europe is moving beyond an era defined by technology adoption toward one defined by governance, resilience, and strategic control.

For organisations, this is not just compliance. It is an opportunity to regain control over fragmented systems, reduce systemic risk, and build foundations for long-term evolution

with partners who make sovereignty practical, not burdensome.

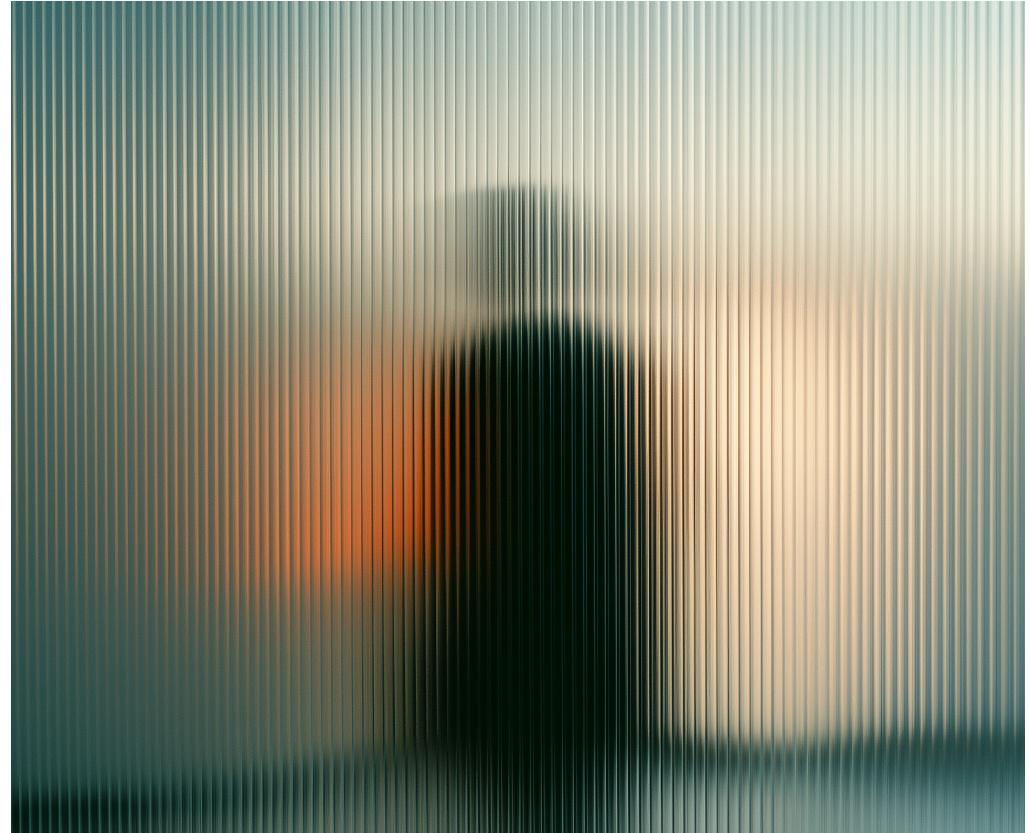
Those that succeed will evolve continuously without losing control of infrastructure, data, or decision-making.

Aruba makes this possible by delivering a unified European stack, from sovereign infrastructure to qualified trust services, from cybersecurity operations to digital identity as one coherent system.

Europe's posture is shifting from writing rules to building capacity. The four regulations defined what trustworthy digital systems must be; instruments such as the proposed Cloud and AI Development Act now ask whether Europe can build them. Aruba sits at that convergence — not waiting for the infrastructure to be built, but already operating it.

It is no longer simply about choosing technology. It is about deciding who governs the digital foundations.

That decision belongs to the organisations Europe is asking to lead the next phase of its digital economy. Aruba's role is to make the architecture that makes the decision possible.



About Aruba

Aruba, founded in 1994, is Italy's Cloud Champion and one of Europe's leading providers of digital infrastructures and platforms based on proprietary assets. The company designs and manages the entire technology stack: from the design and construction of data centers to cloud platforms, from trust and cybersecurity services to connectivity and software solutions that support digital strategies and AI-based applications.

With entirely Italian capital, Aruba serves 16 million users from over 100 countries and operates an infrastructure distributed across 8 data centers, hosting thousands of customers' IT infrastructures.



Copyright © Aruba. All rights reserved.

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it