Managing digital complexity with the European cloud

Deliberate architectures for autonomy, interoperability and strategic control.

aruba.it

Summary

01 | **The evolution of cloud models in the European enterprise** . . . 3
02 | **Interoperability and composable architectures** . . . 5
03 | **European identity and technological freedom** . . . 7
04 | **Compliance by design and governance** . . . 8
05 | **Predictable costs and operational sustainability** . . . 10
06 | **Co-design and the human factor** . . . 12
07 | **Aruba's approach and vision** . . . 15
08 | **Conclusion: cloud as an enabler of strategic control** . . . 18

CHAPTER 01

The evolution of cloud models in the European enterprise

European cloud computing has entered a consolidation phase. After an initial period shaped by the urgency to modernize, organizations now find themselves managing distributed and complex environments and doing so according to criteria that differ markedly from those that guided the first wave of adoption.

The shift is not technological: it is one of maturity. The market has learned that migrating workloads to the cloud is not enough. What matters is understanding which workloads to move, onto which infrastructure, and with what level of control. The question is no longer whether to move to the cloud, but how to govern it in a way that is sustainable, secure, and consistent with the regulatory constraints of the European context.

Many organizations are also reducing their dependence on traditional on-premise data centers, costly to maintain, difficult to upgrade, and increasingly reliant on scarce specialist skills. The move toward next-generation off-premise infrastructure is not a leap but a journey: one that begins with colocation, progresses through lift-and-shift, and arrives, for those with the resources, at full application refactoring.

According to Statista, **the European cloud computing market is expected to surpass €250 billion by 2030, with annual growth exceeding 15%. Globally, more than 70% of organizations have already adopted hybrid or multi-cloud models, confirming that distributed architectures have become the standard of reference**.

The accelerating digitalization of core business processes has driven a fundamental shift in perspective: away from static infrastructure and toward dynamic environments capable of orchestrating distributed workloads, data, and services.

In this context, hybrid and distributed cloud is emerging as the reference architecture for the most mature European organizations.

This evolution raises questions that go well beyond infrastructure. How is risk managed? How are data controlled? How are architectural decisions made over time?
Enterprise architectures today combine on-premise environments for critical workloads, external data centers for resilience, and public cloud for application services. The challenge is not to choose among these models, but to hold them together coherently without letting complexity become a constraint.
It is precisely in this context that managed services take on a central role: they help organizations govern increasingly distributed infrastructures, ensuring operational continuity, security, and continuous adaptation. Through specialized expertise and proactive management models, **managed services reduce complexity, optimize costs, and accelerate architectural evolution**.

For European organizations, data governance and infrastructure localization are becoming central factors in protecting competitiveness and ensuring regulatory compliance.

Cloud is no longer a tactical choice, it is an architectural decision with direct implications for governance, resilience, and technological autonomy.

CHAPTER 02

Interoperability and composable architectures

In the public sector, the shift toward distributed models allows sensitive data to remain on controlled infrastructure while integrating cloud services for analytics and interoperability.

In the enterprise sector, the ability to move workloads dynamically across different environments enables more flexible business strategies and reduces dependency on any single platform.

In this context, the role of the cloud provider changes fundamentally. It is no longer simply a supplier of infrastructure resources, but an enabler of distributed architectures, capable of guaranteeing **interoperability**, **compliance**, and **coherent service orchestration**.

This transition forms the foundation on which resilient, modular, and future-ready digital models are built.

European cloud is not evolving toward centralization, but toward the intelligent orchestration of distributed environments.

In the European digital landscape, interoperability is a structural requirement for ensuring operational continuity and strategic freedom. Organizations operate across distributed environments that must communicate coherently, fragmentation risks compromising efficiency, security, and the capacity to evolve.

In this context, composable architecture emerges as the reference model for building modular and adaptable ecosystems. The goal is not to eliminate complexity, but to govern it, transforming it into a design element. Data, applications, and services are orchestrated across an infrastructural continuum that integrates diverse environments in a coherent way.

The real challenge for CIOs and CTOs is no longer integrating isolated systems, but designing technology ecosystems capable of evolving over time. This means adopting models that allow new technologies to be introduced while protecting existing investments and reducing technical debt.

Composable architectures introduce a modular paradigm in which **resources and services become reusable, dynamically orchestrable components**. This approach enables continuous adaptation to new business requirements, shifts in demand, and regulatory change while maintaining operational coherence.

Market analysis based on Statista data and other research bodies indicates that **more than 60% of European companies consider interoperability between platforms as one of the primary criteria when selecting cloud solutions**.
This confirms that interoperability has become central to IT strategy in Europe's highly regulated, multi-actor environment, a strategic lever for long-term **resilience** and **autonomy**.

Interoperability means designing open systems capable of evolving without constraints and integrating innovation without friction.

CHAPTER 03

European identity and technological freedom

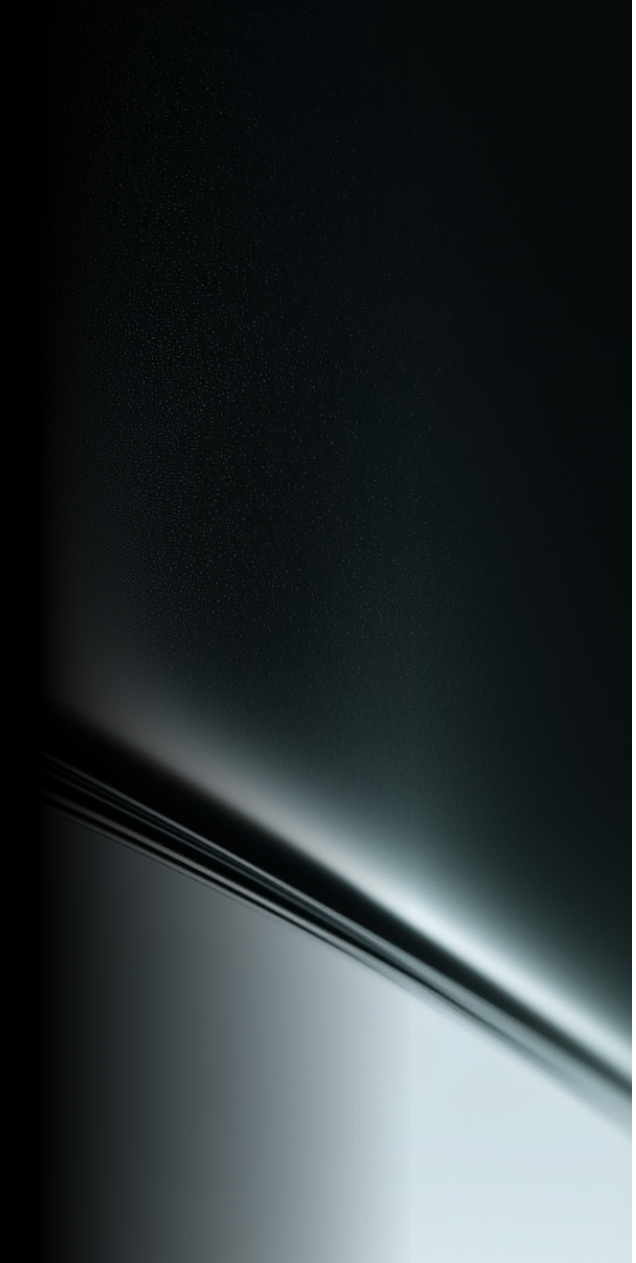
In the enterprise cloud debate, the question of European identity is gaining strategic weight, not as an abstract principle, but as a concrete factor in governance, control, and autonomy. Provider jurisdiction, data localization, and operational models directly shape the architectural choices of organizations. They have become fundamental levers for ensuring transparency, regulatory compliance, and technological freedom.

Leading European analyses indicate that **more than 55% of companies consider data control and regulatory compliance as determining factors in their choice of cloud provider**. This signals that the issue is not merely regulatory, it is increasingly strategic.

The risk of technology lock-in is one of the most significant concerns facing organizations today. Excessive dependency on a single provider can limit the capacity for evolution and constrain future choices.

By contrast, models built on open standards and workload portability preserve decision-making autonomy and strategic flexibility. A genuinely European approach, one that favors open, interoperable, and distributed models in which control is not concentrated but balanced across different infrastructural layers, puts organizations in a position to select and integrate diverse solutions while retaining control, and to remain competitive through the ability to adapt more rapidly to market shifts and technological evolution.

European identity means **autonomy** without sacrificing innovation.



CHAPTER 04

Compliance by design and governance

In the European digital context, compliance can no longer be treated as an activity that takes place downstream of technology processes. The evolving regulatory landscape, spanning data protection, cybersecurity, operational resilience, and critical infrastructure management, requires organizations to embed regulatory requirements directly into the design of cloud architectures.

This is the principle of **compliance by design**: building infrastructure and operational models that incorporate security, traceability, and control from the outset.

For CIOs and CTOs, this represents a paradigm shift. Cloud governance is no longer simply about resource availability or workload efficiency, it becomes a structural element of digital strategy. Architectures must ensure visibility over data flows, segregation of sensitive information, traceability and auditability of processes, and the capacity to respond to incidents. In short, **compliance becomes an intrinsic dimension of system quality**.

The hybrid and distributed cloud model introduces growing complexity: workloads traverse different environments, data resides across multiple jurisdictions, and platforms integrate continuously. Governance therefore demands tools and models capable of maintaining coherence and control without slowing innovation.

By design compliance makes it possible to balance operational agility with regulatory rigor reducing the risk of costly and disruptive remediation.
This enables organizations to navigate the shared responsibility model of cloud effectively, mitigating the challenges of multi-cloud management and internal skills gaps while sustaining effective, scalable governance.

The skills gap deserves particular attention. Research across the European market indicates that more than 50% of organizations report a shortage of advanced cloud competencies, a factor that often leads teams to concentrate on technical operations at the expense of strategic governance.

There is also a growing imperative to make governance measurable and verifiable over time. Organizations must be able not only to implement controls, but to demonstrate their effectiveness through audits, reporting, and continuous monitoring tools. This requires platforms that natively integrate compliance functionality, narrowing the gap between design and operations and making control an integral part of the application lifecycle.

For markets such as the public sector, compliance carries institutional responsibility. The management of critical data, health, fiscal, judicial, infrastructural, demands strong guarantees of integrity, availability, and protection. Private enterprises face analogous challenges, particularly in regulated sectors such as finance, energy, and telecommunications. In both cases, the ability to demonstrate compliance becomes a factor of trust with citizens, clients, and stakeholders.

Another key dimension of modern governance is the ability to automate controls and policies. Cloud architectures designed with embedded compliance logic can apply security and management rules uniformly, regardless of the environment in which workloads reside. This reduces manual errors, improves traceability, and enables rapid adaptation to new regulations.

A concrete example: organizations that implement centralized identity and access management across multi-cloud environments can maintain consistent control over users and privileges, ensuring traceability, auditability, and protection of sensitive data. Similarly, designing resilient and redundant infrastructure makes it possible to meet operational continuity requirements without sacrificing performance or scalability.

These scenarios show that integrated governance is not an operational constraint but a deliberate design choice. Embedding compliance into architectural logic means adopting a model in which **control**, **security**, and **technological evolution** coexist from the moment of design.

Effective compliance does not constrain innovation, it makes innovation **sustainable**.

CHAPTER 05

Predictable costs and operational sustainability

Cloud transformation is often presented as a journey toward flexibility and scalability.

Yet for CIOs and CTOs, one of the most pressing concerns remains economic sustainability over the medium and long term.

Cloud adoption is not only a technology decision, it is a financial and operational one with direct implications for budgeting, governance, and strategic planning. In this context, cost predictability becomes a fundamental requirement for continuity and control.

Research across the European market indicates that **more than 45% of companies cite cost management as one of the primary challenges in cloud adoption**, pointing to the need for more predictable and transparent models.

The consumption-based pricing models typical of public cloud have introduced variable spending dynamics that, if ungoverned, can generate overspending or planning difficulties. Organizations frequently find themselves balancing the need for flexibility with the imperative to maintain cost visibility and stability. This has pushed many enterprise and public sector organizations toward hybrid architectures, where dedicated environments and capacity-guaranteed models coexist with on-demand resources.

A further challenge is the growing need to correlate IT costs with the business value they generate. Monitoring spend alone is no longer sufficient: organizations must understand how cloud resources contribute to performance, innovation, and service quality. This requires advanced cost management tools and closer integration between IT and finance functions in a logic increasingly oriented toward FinOps.

Operational sustainability also encompasses the full infrastructure lifecycle. Migration, integration, maintenance, and evolutionary management are all cost components that must be evaluated systemically.

An architecture designed to reduce operational complexity helps contain indirect costs and improve the efficiency of IT teams.

For public administrations, cost predictability is closely tied to budget constraints and accountability requirements. Infrastructure decisions must ensure transparency and continuity, avoiding financial surprises that could compromise planning. Private enterprises, similarly, require economic models that allow IT spend to be correlated with business outcomes, supporting sustainable investment decisions.

The sustainability of cloud is not measured in unit cost alone, but in the capacity to plan for evolution.

A further dimension is continuous resource optimization. Dynamic workload monitoring and right-sizing logic enable organizations to align infrastructure with real operational needs, eliminating waste and improving overall efficiency.
This approach transforms cost management from a periodic exercise into a continuous, integrated process.

CHAPTER 06

Co-design and the human factor

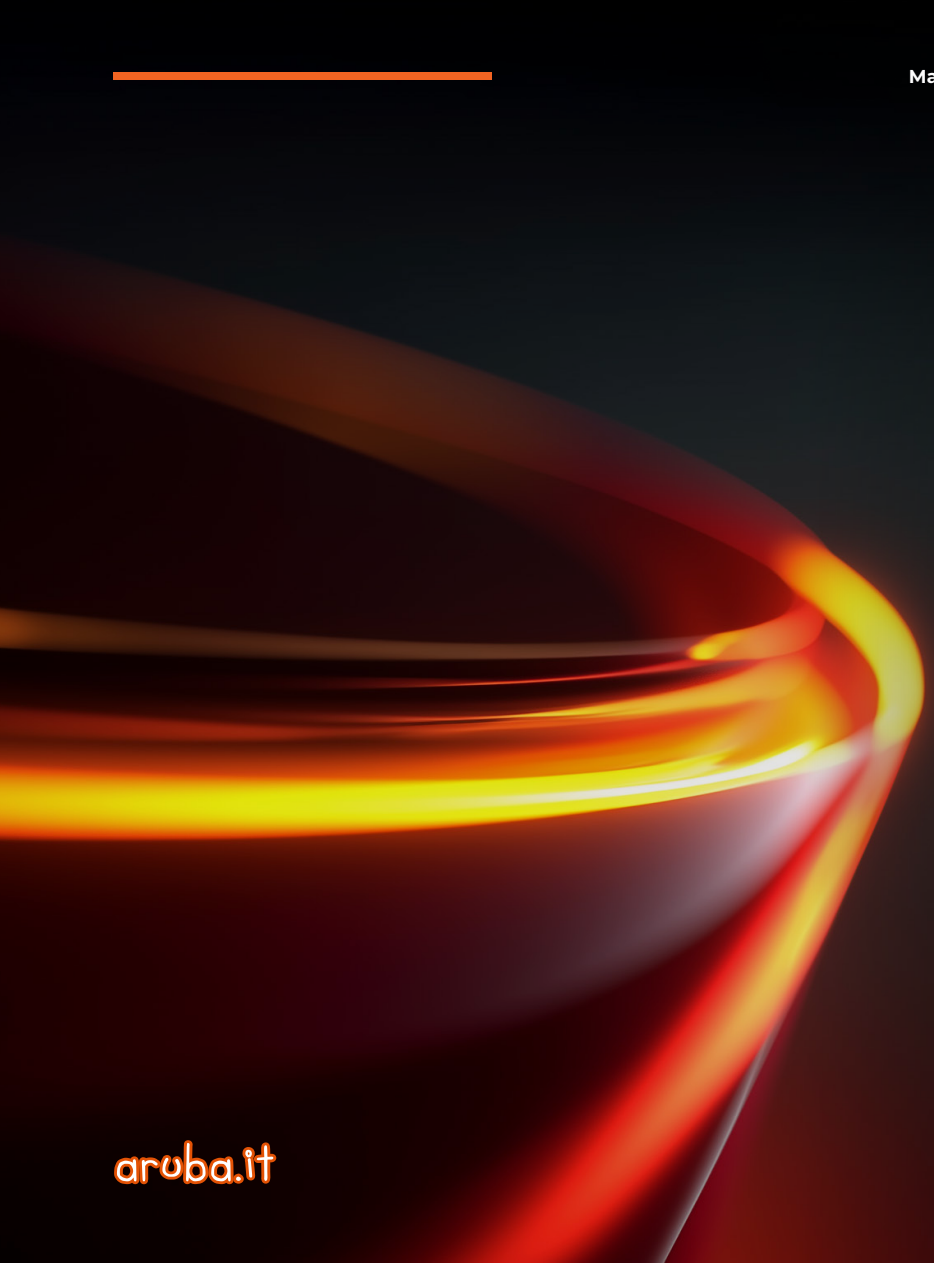
The increasing complexity of cloud architectures makes standardized approaches to infrastructure design progressively less effective. Organizations operate within specific regulatory constraints, technology legacies, and business objectives. In this context, the value lies not only in the technology adopted, but in the **capacity to design solutions that genuinely address real-world requirements. This is where co-design becomes a strategic lever.**

Co-design is a model of shared architectural development in which client, provider, and partners collaborate from the earliest stages. It is not about customizing existing solutions, but about building ecosystems that are coherent with strategic priorities. This approach reduces the risk of misalignment, improves decision quality, and accelerates adoption.

A defining characteristic of co-design is the ability to **anticipate critical issues**. Continuous dialogue between all parties allows technical, regulatory, and operational constraints to be identified before they become problems, reducing implementation time and cost, and making the decision-making process more robust and informed.

The **human factor is equally central**: skills, relationships, and collaboration are key determinants of success. In a context of rapid change, the capacity to work in an integrated way, across internal and external teams, becomes a **concrete competitive advantage**. Shared design also strengthens governance. When architectural choices emerge from a structured collaborative process, the organization retains greater control over future evolution and reduces dependency on rigid, externally imposed models.

Effective cloud is not purchased:
it is designed together.



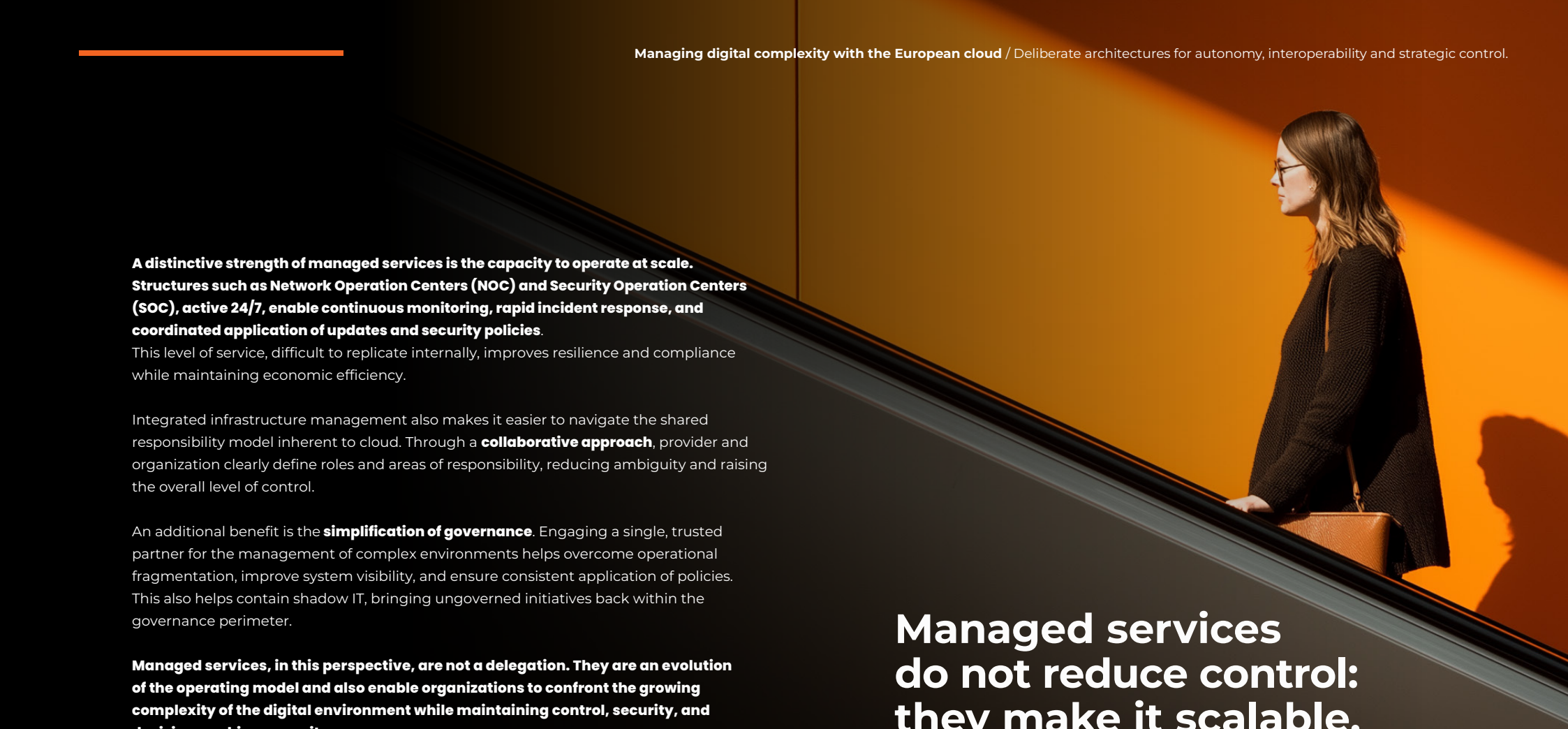
Managed Services: from Operational Complexity to Advanced Governance

As cloud architectures become increasingly distributed and hybrid, the operational management of infrastructure becomes one of the primary sources of complexity. In this context, **managed services represent a strategic lever for transforming technical complexity into governance capability**.

The managed services model rests on a core principle: separating operations from governance. Organizations retain strategic control over data, architectures, and decision-making processes, while delegating to a specialized partner the day-to-day management of infrastructure, security, and operational continuity. This allows internal resources to be reallocated toward higher-value activities, while simultaneously reducing operational risk.

According to MarketsandMarkets, **the global managed services market is expected to reach approximately $355 billion by 2027**, confirming a structural trend: organizations are no longer seeking technology alone, but sustainable operational models to govern it.

In the cloud paradigm, the role of the Managed Service Provider evolves significantly. It no longer simply delivers services, but assumes **proactive** responsibility for infrastructure management, helping to prevent critical issues, ensure continuity, and support system evolution. This is particularly relevant in multi-cloud environments, where technological fragmentation increases the complexity of maintaining control.



A distinctive strength of managed services is the capacity to operate at scale. Structures such as Network Operation Centers (NOC) and Security Operation Centers (SOC), active 24/7, enable continuous monitoring, rapid incident response, and coordinated application of updates and security policies.
This level of service, difficult to replicate internally, improves resilience and compliance while maintaining economic efficiency.

Integrated infrastructure management also makes it easier to navigate the shared responsibility model inherent to cloud. Through a **collaborative approach**, provider and organization clearly define roles and areas of responsibility, reducing ambiguity and raising the overall level of control.

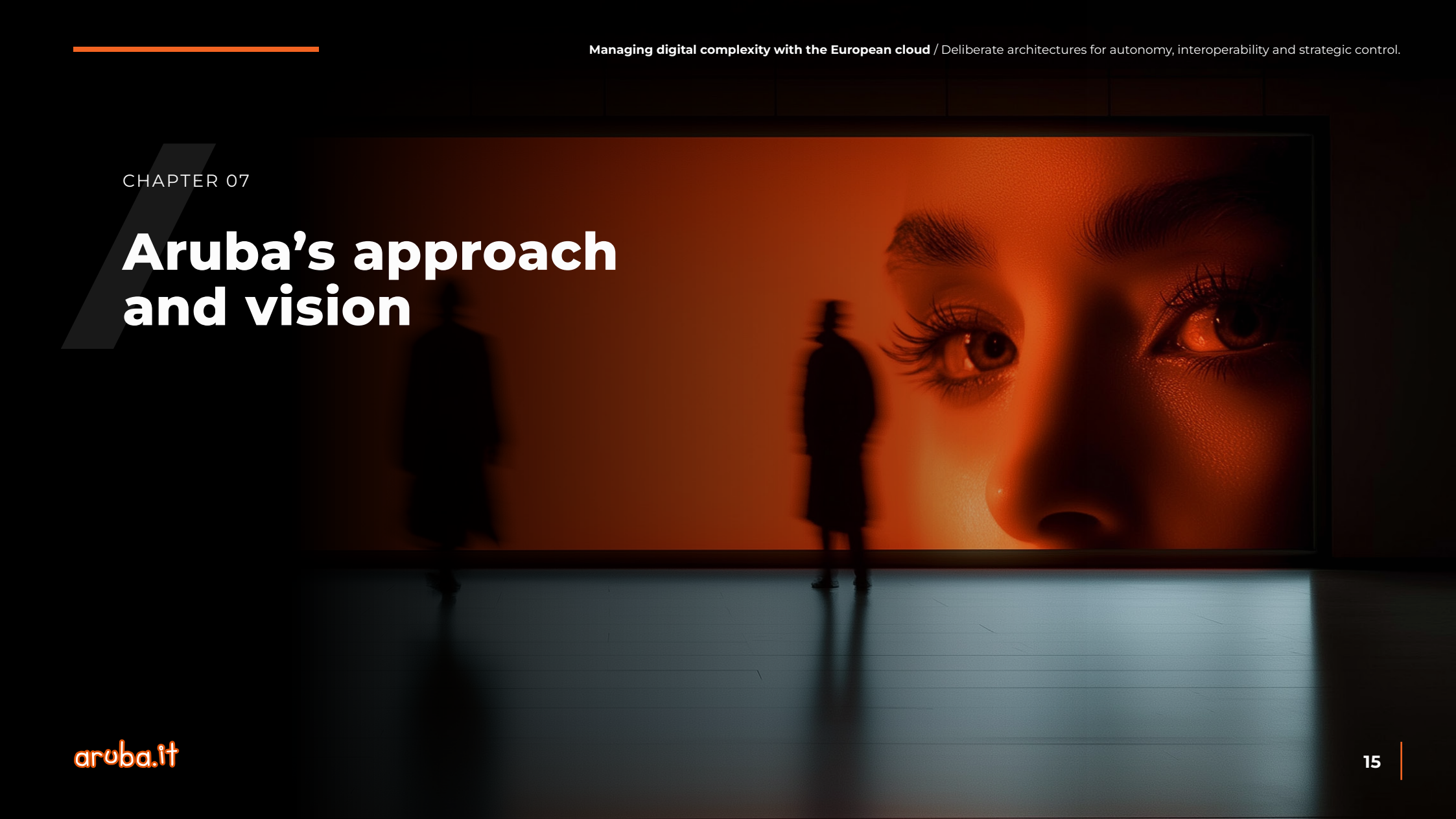
An additional benefit is the **simplification of governance**. Engaging a single, trusted partner for the management of complex environments helps overcome operational fragmentation, improve system visibility, and ensure consistent application of policies. This also helps contain shadow IT, bringing ungoverned initiatives back within the governance perimeter.

Managed services, in this perspective, are not a delegation. They are an evolution of the operating model and also enable organizations to confront the growing complexity of the digital environment while maintaining control, security, and decision-making capacity.

Managed services do not reduce control: they make it scalable.

CHAPTER 07

Aruba’s approach and vision



A cloud provider that limits itself to delivering compute and storage capacity is answering the questions of ten years ago. Today, organizations need a partner who can design alongside them, not simply deliver to them. This is the difference between a vendor and a strategic interlocutor.

Aruba operates across the entire chain: from architectural design to operational management, from physical data centers to connectivity, from cloud platforms to compliance logic. This is not a service catalog, it is a model in which infrastructural, network, and governance decisions are designed coherently, rather than assembled after the fact. What distinguishes this approach is continuity: the same partner who helps design the migration is the one who manages the production environment and is first to identify when something is not performing as expected. In hybrid and distributed architectures, this continuity is not a convenience but it is a structural reduction of operational risk.

Being a European operator, with physical infrastructure in Europe, subject to European jurisdiction, is not merely a matter of geography. It means that when regulations change (GDPR, NIS2, DORA, AI Act), the architectural implications are handled within the perimeter, not negotiated with an extra-European provider. For public administrations and enterprises in regulated sectors, this concretely reduces the compliance burden.

Aruba's approach also integrates co-design logic, helping to reduce the weight of shared responsibility, supporting organizations in operational management, and allowing IT teams to focus on governance and innovation.

aruba.it

EVIDENCE OF ARUBA'S COMPOSABLE CLOUD ARCHITECTURE

European infrastructure at scale
Aruba serves more than 200,000 cloud clients across over 100 countries, from 8 proprietary cloud regions distributed across 6 European countries.

Open standards for reversibility
Built on SECA, standard Kubernetes, and open projects (Liqo, ArubaKube), Aruba's platform ensures workload portability across Aruba environments, hyperscalers, and on-premise infrastructure with no proprietary lock-in.

Hybrid integration and public-sector qualification
Multi-Cloud Link and Hybrid Connect provide direct, dedicated connectivity to AWS, Azure, Google Cloud, and on-premise infrastructure under transparent economics.

Aruba Cloud is qualified for the Italian public administration (ACN QC3, Consip) and is a Gaia-X Board Member, operating as an active node of the Gaia-X Digital Clearing House.

+200K
CLOUD CUSTOMERS SERVED BY ARUBA

8
PROPRIETARY CLOUD REGIONS

+16M
USERS

8
COMPANY-OWNED DATA CENTERS IN THE EU

evidence box

CHAPTER 08

Conclusion: cloud as an enabler of strategic control

The evolution of cloud in the European context cannot be read as a purely technological transformation. It is a transformation of the way in which organizations exercise their own decision-making capacity.

Strategic control means having the freedom to choose: which workload to move, when, to which environment, with which provider. This is not only a question of technology but it is a question of architecture designed to keep options open rather than foreclose them. Interoperability, governance, and cost sustainability are not three separate objectives: they are the three conditions that, together, make complexity governable.

Innovation is not the freedom to do more, it is the freedom to choose better.

A further critical dimension is the speed of decision-making. In competitive and regulated environments, the capacity to adapt rapidly becomes essential. Flexible, well-governed architectures reduce time-to-decision and improve organizational responsiveness.

AI makes all of this more urgent, not simpler. Models operating on sensitive data, distributed infrastructure, and within stringent regulatory frameworks require architectures designed for control. European cloud, in this sense, is not an alternative to innovation, it is the condition for pursuing it sustainably.

In this perspective, **European cloud emerges as strategic infrastructure capable of restoring control, autonomy, and adaptive capacity to organizations**.

Strategic control means transforming complexity into the capacity to choose.

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