



Cybersecurity as Structural Control

A European approach to resilience,
accountability and operational independence.

aruba.it

pr
u
i
s
e

Summary

01 Cybersecurity in an Era of Distributed Control	3
02 The Governance Crisis of Distributed Security	6
03 Cybersecurity as Structural Control	7
04 Secure Growth for Enterprises and SMEs	9
05 From Principles to Capabilities	11
06 The Future of Cybersecurity	15
07 CONCLUSIONS	17

CHAPTER 01

Cybersecurity in an Era of Distributed Control

From digital opportunity to digital exposure

In the early days of digital transformation, digital technologies multiplied opportunities and opened up new ways of living and working. At the same time, risks also became digital: **security moved from the physical world into the digital domain** and focused on guarding well-defined perimeters. COVID-19 pandemic and the rise of remote working increasingly blurred those perimeters. Today, cybersecurity is evolving to reflect how organisations themselves have become digital organisations.

Cybersecurity has moved from a specialised technical domain into one of the defining investment priorities of the digital economy.

This growth reflects a broader management shift. Cybersecurity budgets are expanding because organisations are no longer investing only in defensive tools, but in resilience, response capacity, data protection, cloud governance and board-level confidence. The same technologies driving digital transformation are also reshaping the threat landscape.

The perimeter has dissolved

For years, **security was treated as a specialised function**: important, technical and often complex, but still separate from the core architecture of the business. That separation no longer holds.

Infrastructure is now distributed across cloud platforms, SaaS environments, APIs, remote users, operational systems, third-party providers and increasingly automated processes. The organisation is no longer contained inside a clearly defined perimeter. It operates through a constantly shifting network of dependencies.

Risk now moves across dependencies

This has created enormous flexibility. It has also changed the nature of risk. A vulnerability no longer affects only one system. It can move across identities, workloads, suppliers, applications and customer-facing services.

A problem in one layer can quickly become an operational, regulatory and reputational issue.

In this environment, cybersecurity is not only about preventing attacks, or rapidly recovering from them. It is about preserving the ability to govern digital systems that are always connected, always exposed and increasingly interdependent.

Security must be designed from day one

It has to become part of how digital environments are designed, operated and governed from day one. As cyber threats evolve and regulations reshape accountability, cybersecurity must become structural across the full technology stack, enabling digital integrity, EU data residency, operational control and technology independence.

Europe's shift toward continuous accountability

For European organisations, further pressure comes from EU institutions, which are increasingly focused on building a resilient and secure digital Europe.

Regulations such as NIS2, GDPR, DORA and the AI Act are pushing cybersecurity away from episodic compliance and toward continuous accountability.

Boards are expected to oversee cyber risk. Supply chains must be governed. Operational resilience must be demonstrated. Compliance is no longer a final check. It is becoming an architectural requirement.

Resilience, EU data residency and strategic control are now critical priorities and are firmly placed at the centre of cybersecurity decisions.

Strategic Control is key

Maintaining strategic control over infrastructure, data, jurisdiction and operational accountability is the new frontier.

Where systems run, who governs them, how data moves and who ultimately controls critical dependencies are now strategic questions. This is not about rejecting external ecosystems or global partnerships, which remain strong and structural. It is about ensuring that organisations retain meaningful visibility, authority and accountability over the systems on which they depend.

The control gap is also a skills gap

Cybersecurity demand is increasing faster than many organisations can staff internally. The global cybersecurity workforce continues to grow, but the shortage

of skilled professionals remains significant, especially in Europe. This reinforces the strategic value of integrated operating models, managed security capabilities, automation and clear governance: enterprises need resilience even when specialist skills remain scarce.

From market growth to structural control

The market is expanding because risk is spreading **across cloud platforms, SaaS environments, identities, supply chains, AI-enabled workflows and critical business services.**

More spending does not automatically create more control. For enterprises, the real challenge is **whether security investments can be translated into a coherent operating model: one that connects infrastructure, data, identity, compliance, detection, response and recovery.**

This is the context in which cybersecurity becomes structural control.

CHAPTER 02

The Governance Crisis of Distributed Security

Complexity accumulates faster than accountability

Control becomes harder when every new risk generates another tool, every new platform introduces another provider, and every new regulatory requirement adds another governance layer.

Over time, organisations may accumulate technologies and even capabilities, but not necessarily coherence. Individually, these components may work well. Collectively, they can create a fragmented operating model in which infrastructure, cloud, identity, compliance and security operations are managed through different teams, contracts and accountability structures.

Visibility may increase, but responsibility becomes harder to trace.

CHAPTER 03

Cybersecurity as Structural Control

Structural control starts with architecture

This is where Aruba's approach starts: **the answer cannot simply be more layers of security. If fragmentation is the problem then the answer has to be architectural. This is the logic that elevates Cybersecurity to Structural Control.**

Security is not treated as a separate layer placed above infrastructure or cloud platforms. It is part of the architecture that allows organisations to govern their digital environments while preserving digital integrity across data centres, cloud platforms, connectivity, identities, compliance and trust services.

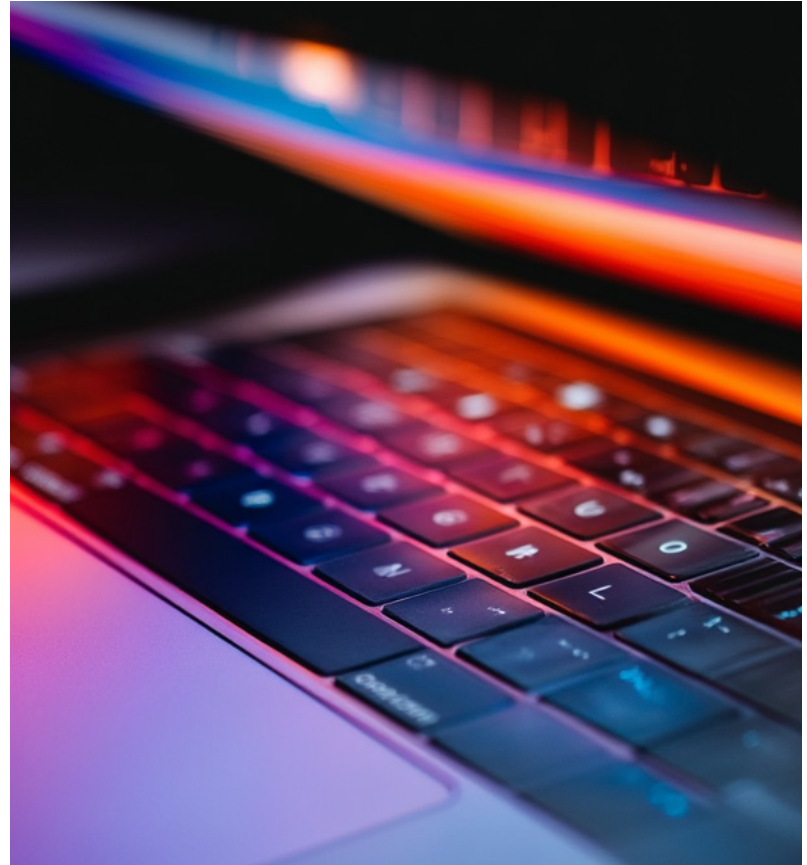
Resilience depends on knowing who controls what, where systems operate, how responsibilities are distributed and how quickly the organisation can act when something happens.

Aruba's approach to coherent digital environments

Aruba's positioning reflects this. **As a European provider built on proprietary infrastructure, Aruba connects data centres, cloud and trust services within a broader model of control.** The point is not to build closed ecosystems. The point is to reduce hidden dependency risk while preserving the ability to evolve. The value is not only in individual services, but in the coherence of the environment they support. Our commitment to open standards and transparent architecture ensures **that control remains with the organisation, avoiding proprietary lock-in.**

European compliance as an operating discipline

This also changes the meaning of compliance. Security cannot be just a stack of technology features and layers, and compliance cannot be reduced to a checklist or reporting exercise. **In a regulatory environment shaped by NIS2, GDPR, DORA, the AI Act and the Cyber Resilience Act,** especially as connected products and digital components become part of critical business environments, organisations need systems that make oversight, traceability and resilience part of the operating model itself. The strategic objective is therefore not simply stronger protection. It is the creation of digital environments where security, resilience and governance reinforce one another. **Control is not created by adding complexity. It is created by reducing fragmentation.**



CHAPTER 04

Secure Growth for Enterprises and SMEs

Cybersecurity now extends across business ecosystems

Its scope now includes customer platforms, supply chains, partner ecosystems and digital transactions.

For both enterprises and SMEs, cybersecurity is therefore becoming a business decision. It protects the integrity of digital transformation by helping organisations safeguard people, data, services, customers, brand reputation and business continuity. In this sense, cybersecurity is not only about reducing exposure. It is about creating the confidence required to grow securely and sustainably.

End-to-end protection remains essential, but customers increasingly need cybersecurity to support supplier confidence, contractual accountability, auditability and customer trust.

A secure infrastructure is not only a technical asset. It becomes a business platform through which organisations can exchange data, deliver services, prove compliance and preserve operational credibility.

Each enterprise stakeholder has a different control question

This also changes the way cybersecurity is evaluated. **CISOs** need to reduce risk and improve response. **CIOs** and **CTOs** need secure and interoperable foundations. **Risk and compliance leaders** need evidence and traceability. **Procurement and legal teams** need clarity on vendor responsibility, data residency and third-party dependencies. **Boards** need confidence that cyber risk is being managed in a way that protects continuity, reputation and growth.

A model designed for adoption

The challenge for many organisations is not only choosing stronger security technologies. It **is adopting cybersecurity in a way that is scalable, repeatable and aligned with their operating model.**

SMEs often need access to trusted expertise without unnecessary complexity. Enterprise customers need services that can integrate into broader organisational, technical and governance environments.

Aruba's approach is designed around this reality. **Our cybersecurity services are built to be modular, repeatable and accessible across different levels of maturity**, helping customers make security easier to integrate into everyday operations and long-term growth.

Different needs for different customers

Operational autonomy varies from customer to customer. Some want to delegate cybersecurity operations to a trusted provider. Others want to retain direct control and integrate security services into their own internal processes.

For this reason, Aruba structured its services in two complementary models. The **Managed/SaaS model** is designed for customers that want Aruba to operate the service on their behalf. The **Self-Managed/PaaS model** is designed for customers that want more autonomy within an Aruba-hosted environment.

This dual-flavour approach allows the same strategic principles to serve different customer profiles. **SMEs can access reliable cybersecurity services in a simpler and more sustainable way. Enterprises can adopt services that support greater integration, scale and control.**

Trust as the foundation for growth

Structural control connects enterprise security and B2B trust. It helps organisations protect their digital business while preserving the ability to collaborate, integrate and evolve. As digital ecosystems become more automated, this trust increasingly depends on verified identities, reliable certificates, authentic content and traceable interactions. For Aruba, the value is not only in protecting individual layers of the stack. It is in **making cybersecurity easier to adopt, to govern and more directly connected to business growth.**

CHAPTER 05

From Principles to Capabilities

Structural control must become operational

This principle becomes meaningful only when operational capabilities are tangible and proven in the field.

At Aruba, we are our own first and largest cyber client, which means we know cybersecurity must be designed and operated around the capabilities enterprises need to govern distributed environments in practice.

We apply our principles and capabilities across all our environments, so we test them in the same conditions our customers face.

What are these capabilities? **Aruba delivers European cloud security solutions, open architectures where applicable, and end-to-end cyber capabilities that strengthen its core offerings.**

Operational resilience

Modern cyber risk is continuous, so monitoring and response must be continuous as well. **Managed SOC and MDR services**, integrated with security orchestration capabilities, **support this need by helping organisations detect threats, coordinate response and maintain visibility across complex environments.** The goal is not only faster detection. It is stronger continuity.

Identity and digital trust

As organisations become more automated, identity is no longer limited to people. **It includes certificates, APIs, machines, services and automated workflows. Machine identities are becoming as critical as human identities, because they determine which systems, services and automated processes can act, exchange data and make decisions.**

They need to be governed, renewed, authenticated and traced. Certificate lifecycle management and trust services become essential parts of the security architecture because they protect the reliability of digital interactions.



In the AI era, trust also extends to content: organisations will increasingly need to verify not only who or what acted, but also whether digital content, data and machine-generated outputs can be trusted.

Infrastructure and cloud security

As workloads move across hybrid environments, infrastructure becomes inseparable from cybersecurity strategy.

Organisations need secure foundations that are interoperable, scalable and aligned with their governance requirements.

This is where Aruba's broader ecosystem becomes strategically relevant: security is connected to the infrastructure layer, not detached from it.

Compliance and accountability

Enterprises need to demonstrate resilience, traceability and control on an ongoing basis. That requires monitoring, identity, infrastructure visibility and governance to work together.

Compliance by design is valuable because it turns regulatory pressure into an architectural discipline.

AI-era security

AI is changing both attack and defence. **Automated attacks, synthetic identities, machine-generated deception and AI-driven operations increase the speed and complexity of risk.**

They also create a new trust challenge: organisations will need ways to verify the origin, integrity and reliability of machine-generated content, decisions and interactions. At the same time, AI can strengthen detection, analysis and response.

From isolated tools to a security operating model

Together, these capabilities support a simple proposition. Enterprises do not need more isolated tools. They need integrity guaranteed across infrastructure, identity, resilience, compliance and response, connected capabilities that turn security into an operating model.

Cybersecurity becomes the architecture that allows digital transformation to remain governable.

EVIDENCE OF ARUBA'S CYBERSECURITY OPERATING CAPABILITY

SOC and managed detection at scale

Aruba operates a 24x7 Security Operations Centre with Managed Detection and Response (MDR) and Extended Detection and Response (xMDR) services, protecting more than 5.4 million customers across the European footprint.

NIST CSF alignment and certifications

Aruba's security posture is aligned to the NIST Cybersecurity Framework, with ISO 27001 certification, ACN QC3 qualification, and dedicated capabilities for vulnerability assessment, penetration testing (VAPT), web application protection (WAP), and anti-DDoS.

Cybersecurity as Aruba's own first product

The same security operations that protect Aruba's enterprise customers are the operations Aruba runs to protect itself, 1.6 billion signatures, 9 million PEC mailboxes, and Italy's national trust infrastructure depend on this maturity every day.

+5.4M

PROTECTED CUSTOMERS
ACROSS EUROPE

1.6BN

PROTECTED ENTERPRISE
CUSTOMER SIGNATURES

+16M

USERS

9M

PROTECTED ENTERPRISE
PEC MAILBOXES

evidence box

CHAPTER 06

The Future of Cybersecurity

Governance and independence will define the next phase

We are entering a new digital transformation era: governance and technology independence will matter more and more.

The future of **Cybersecurity will not be defined only by stronger defence. It will be defined by the ability to preserve strategic control as digital environments become more automated, distributed and interdependent.**

Our digital future is not only about defence but will also be about recovery. How we defend, how we protect and how we recover are all central to Europe's next phase of cybersecurity.

AI will reshape both attack and defence

Because of AI, attacks will become faster, more adaptive and harder to attribute.

Defence will become more predictive, automated and dependent on real-time analysis. At the same time, AI systems themselves will need to be monitored, authenticated and governed, with clear accountability for the identities, data sources and automated decisions they rely on.

Identity will become the control plane

As machine identities, APIs, delegated agents and autonomous workloads multiply, organisations will need stronger ways to verify authority and attribute actions.

Trust will depend on knowing not only who did something, but which system, service or automated process acted, under what authority, and with what accountability. Over time, this trust layer will also need to prepare for **post-quantum cryptography**, as enterprises begin to assess how today's encryption, certificates and long-term data protection strategies will evolve in a quantum-ready world.

Resilience will include jurisdiction and infrastructure governance

Organisations will evaluate **their security posture not only through products and tools, but also through infrastructure governance, jurisdiction, data control and operational independence.** Where systems run and who governs them will increasingly shape security decisions.

Regulation will reinforce this shift. **Cybersecurity, compliance, infrastructure strategy and operational resilience will continue to converge.** Architecture decisions will become governance decisions.

Cloud decisions will become cyber decisions. Artificial Intelligence decisions will become accountability decisions.

Aruba's position for the next phase

This is the environment Aruba is positioning for: **European infrastructure, interoperability, compliance by design, operational resilience and integrated governance.** It means providing cutting-edge technologies and managing a full digital stack that leaves you firmly in the driver's seat.

Cybersecurity is no longer only the function that protects digital transformation from disruption. **It is becoming the discipline that enables transformation, enhances resilience and empowers organisations to evolve through strategic control.** The future advantage will belong to those that can evolve without losing control.

CHAPTER 07

Conclusions

Cybersecurity is no longer only a matter of exposure. It is a matter of interdependence, governance and control.

As digital environments become distributed across cloud platforms, SaaS services, APIs, identities, suppliers and AI-driven systems, a cyber event can quickly move across the business ecosystem and affect operations, compliance, reputation and growth.

Many organisations have responded to this complexity by adding more tools, controls and specialised capabilities. But **more security does not automatically create more control.**

When technologies, providers, responsibilities and regulatory requirements accumulate without a coherent operating model, visibility may increase while accountability becomes harder to trace.

Fragmentation therefore becomes one of the central cybersecurity challenges of the next enterprise phase.

This is why cybersecurity must become structural. It must be part of how digital environments are designed, hosted, operated and governed. The objective is no longer only to prevent attacks or respond to incidents. It is **to preserve digital integrity: the ability**

to protect people, data, services, customers, brand reputation and business continuity while enabling organisations to innovate, comply and grow with confidence. For European enterprises and SMEs, this shift is especially relevant.

Regulation, sovereignty, infrastructure governance and supply-chain control are becoming inseparable from cybersecurity decisions.

Where services run, who operates them, how dependencies are managed and how accountability is demonstrated are now business questions as much as technical ones.

Aruba's approach responds to this need through cybersecurity as structural control.

By combining EU-based foundations, Aruba-hosted services, open technologies where possible, and flexible Managed/SaaS or Self-Managed/PaaS delivery models, Aruba helps organisations move from fragmented protection to secure, governable and scalable digital environments.

Cybersecurity is becoming the foundation that allows digital transformation to remain trusted, compliant, resilient and sustainable, while enabling organisations to keep growing without losing control.

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