Your Digital Presence in the AI Era

From storefront to Trusted Digital Presence.

aruba.it

signal

INTRODUCTION

Businesses are entering a new phase of digital evolution. This phase is certainly AI-driven (though we are still in its very early stages), or should we say AI-disrupted?

One of the first and most visible effects of AI has been the rise of zero-click behaviour, which undermines the website's dominant position as the main place where discovery, engagement, and transactions begin.

A second trend, I believe linked to AI as well as to human fatigue, but certainly measurable, is the gradual decline of social media as the main digital agora where people discuss and exchange ideas.

Lastly, a third trend, probably more distant in time: the gradual shift from smartphones towards AI wearables.

The assumption that we interact on social forums and use screens (PCs or mobile phones) to search for answers and knowledge is faltering: AI answer engines, agentic interfaces, and zero-click behaviours are changing how customers find information and make decisions, while regulation, cyber risk, and digital identity requirements are raising the value of trust and control across the whole digital stack.

This does not spell the decline of the website, whose value remains essential, but it does mean rethinking the model built around it.

In the AI era, the site's value rises to that of authoritative source, secure place of transaction, and trust anchor behind a broader digital presence. Websites will become less of a standalone digital storefront (or info booth) and turn into digital presence hubs that are machine-readable, protected, compliant, authoritative, and verifiable.

The website-centric era gives way to the era of Trusted Digital Presence.

Aruba has been building the infrastructure behind organisations' digital presence for three decades.

The AI era redefines what that infrastructure must do. This paper sets out how, and what businesses should do about it.

Summary

01 | **What is happening now** 5

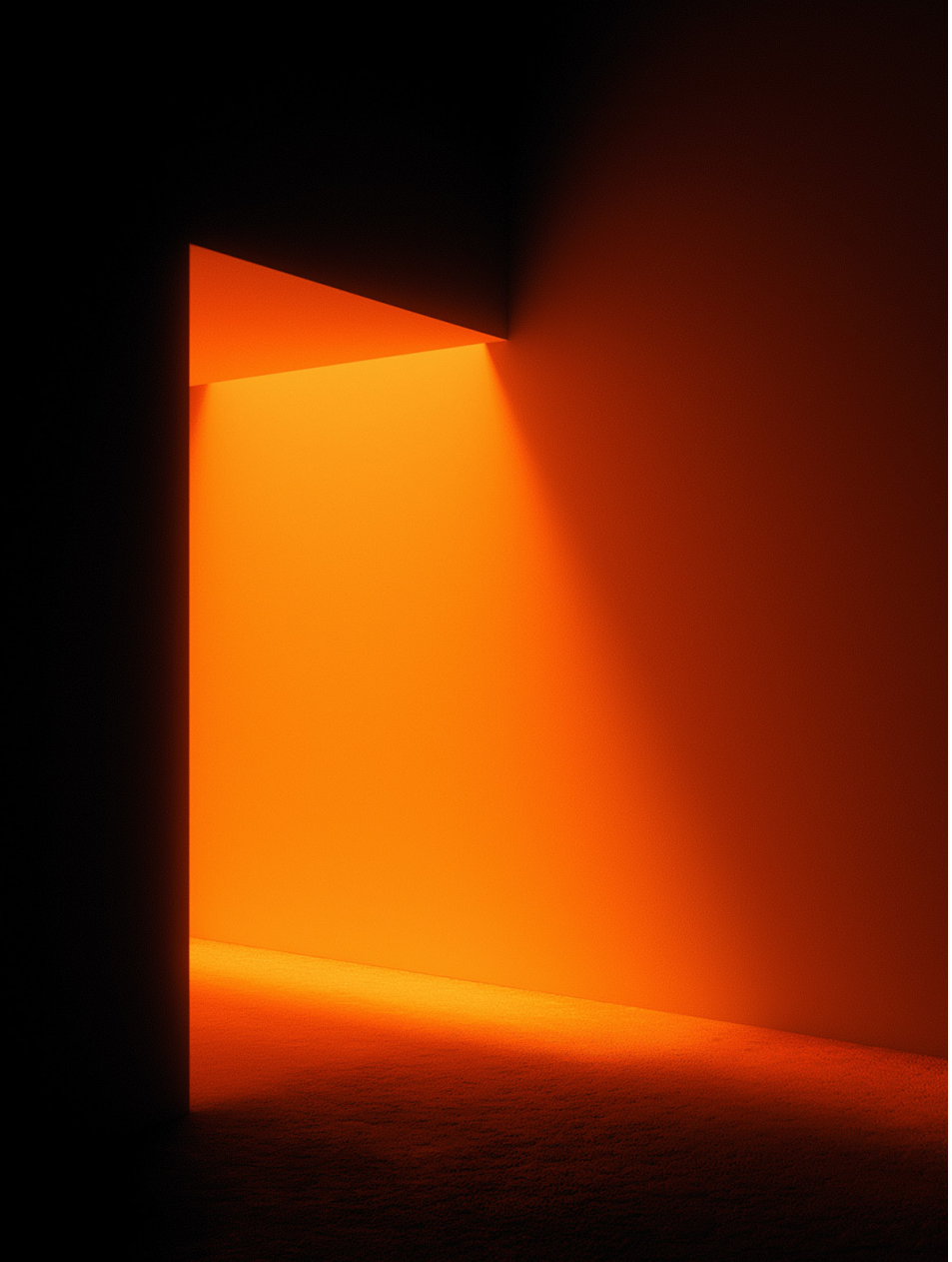
02 | **What we are witnessing** 6

03 | **What this means for businesses** 7

04 | **What actions to take now** 8

05 | **How Aruba can help** 10

06 | **Beyond zero-click** 11



CHAPTER 01

What is happening now

We are entering a new phase of digital transformation. The destinations are not yet in focus, but the direction the world is taking certainly is. In times of change, reading that direction is the first step. The second is turning it into deliberate choices, and into new positioning. Disruptions bring opportunities for those best positioned and most aware. So let's look at the directions our digital world is taking.

First, discovery is moving from link-based browsing to AI-mediated answers. Industry research on zero-click behaviour shows that visibility is increasingly determined by whether a brand is trusted and machine-readable inside AI answer systems, more than by its ranking on a search results page.

Search engines ranked pages. AI ranks authority. SEO was, and remains, central, but the new paradigm calls for a rethink of content, structure, and strategy.

Meanwhile, overall engagement on social media is declining, reducing the ability of traditional channels to intercept visitors and route them to a website. Search and social, the two engines that fed website traffic for two decades, are both delivering less, at the same time.

While these shifts are not under your control, your organisation's digital presence is. That makes its credibility (and its machine-readability) a strategic priority.

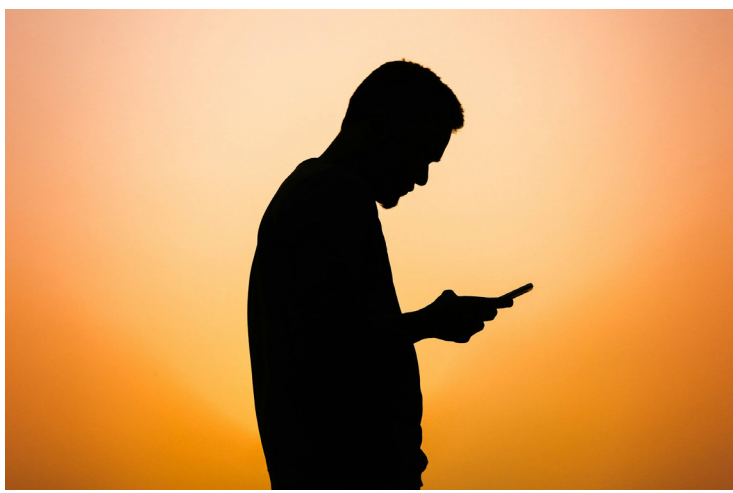
Second, digital environments are becoming more distributed and harder to govern. Organisations will increasingly operate across cloud platforms, SaaS applications, APIs, connected devices, automated workflows, and AI-driven systems.

In that context, data integrity and trust are factors you engineer in from the start, across infrastructure, identity, cybersecurity, and communications, not layered on later.

In this new phase, brand alone is not enough, because a brand claim carries no weight with a machine.

Third, regulation is changing the buying criteria for digital services. eIDAS 2.0, NIS2, DORA, and the AI Act are pushing organisations toward architectures that can prove who acted, under what authority, on what infrastructure, and with what safeguards.

Compliance is moving from after-the-fact verification to an architectural requirement from the start.



CHAPTER 02

What we are witnessing

In practice we are heading towards a redefinition of digital presence. For years, businesses invested in websites mainly as destinations: attract traffic, present products, convert visits into business. That model still matters, but it is becoming less central to how customers find and compare, because many journeys now begin and end in AI interfaces that summarise, compare, and recommend without requiring a click.

As a result, the role of the website is changing. It must also become the verified source behind AI answers and the point of reference for authoritative product and brand information. In many cases it is also where higher-value actions still happen: authenticated access, ecommerce, document exchange, support, onboarding, signing, and legally significant transactions.

At the same time, trust is becoming a practical, day-to-day matter. A cloned website, a spoofed email domain, or a fake invoice can now be produced in minutes, and customers, suppliers, and increasingly AI systems all need a way to tell the real business from the imitation. That is why **cybersecurity, trust services, brand protection, and digital identity are converging: together, they are what lets an organisation keep control of its digital interactions as fraud gets cheaper and faster to produce**.

CHAPTER 03

What this means for businesses

If you are wondering "Do we need a website?", you are asking the wrong question.

The question that matters is how to keep your digital presence credible, secure, and governable in an AI-mediated world. The real issue is control, and how to keep it as you evolve.

Content must work for AI systems as well as people
Product, service, and corporate information has to be authoritative, current, and structured so that machines can retrieve and interpret it.

Digital presence must be protected as a trust surface
Domains, DNS, email, websites, and public-facing digital assets form part of the organisation's visible identity (and a direct attack surface for impersonation, phishing, and fraud).

Value shifts to transactions, and transactions demand governance.
If AI can summarise a generic web page, the defensible value of a website shifts toward the transaction itself: secure portals, ecommerce, onboarding, certified communications, signatures, and service workflows. And it is exactly there that identity assurance, legal validity, auditability, and jurisdictional control stop being compliance costs and become business enablers, especially in Europe, where regulation increasingly shapes how organisations buy and design digital systems.

In short, digital presence is shifting from storefront-centric to trust-centric. The organisations that win will be those with the most credible and secure digital presence, under their own control, across AI, web, identity, and transaction layers.

That is what Trusted Digital Presence means.

CHAPTER 04

What actions to take now

A practical response starts with reframing digital presence as an operating model rather than a website project: one that carries your strategic vision and market positioning as much as your technical details and pricing.

1

UPGRADE THE WEBSITE'S ROLE

Treat the website as the authoritative source of truth for products, services, pricing logic, policies, credentials, and brand values. Make it clear, structured, up to date, and built to support both human visitors and Artificial Intelligence retrieval layers.

2

PRIORITISE SECURE SERVICE ENDPOINTS

Shift investment from brochure pages alone toward ecommerce, customer areas, authenticated workflows, calculators, document exchange, booking, support, and other functions that create direct utility.

3

PROTECT THE DIGITAL EDGE

Strengthen control over domains, DNS, SSL certificates, email, and brand assets, and monitor for impersonation and abuse. In an AI era, public trust can be lost as quickly through a fake domain or spoofed communication as through a compromised application.

4

EMBED CYBERSECURITY AND COMPLIANCE BY DESIGN

Security, traceability, and resilience belong in hosting, cloud, identity, and communications from day one.

5

PREPARE FOR IDENTITY-CENTRIC TRANSACTIONS

As wallets, signatures, certified delivery, and machine identities become more relevant, organisations need digital processes that can verify who is acting, what is being approved, and how authority is delegated.

CHAPTER 05

How Aruba can help

Aruba is well positioned because this shift calls for an integrated architecture rather than a single product.

Aruba provides the trusted digital infrastructure that powers digital presence: **hosting, website building, ecommerce, cybersecurity, trust services, digital identity, brand protection, and infrastructure** under European jurisdictional control.

These are assets under your control, operated by a European provider, under European law.

That means Aruba can support businesses on several levels.

AS THE INFRASTRUCTURE LAYER

Aruba provides the foundation on which digital presence takes shape and evolves: hosting, cloud, and domains, with increasing relevance for AI-ready, jurisdictionally controlled, and compliance-aware workloads.

AS A CYBERSECURITY AND BRAND PROTECTION PARTNER

Aruba helps protect the visible edge of the business across websites, domains, applications, certificates, and communications.

AS A TRUST SERVICES AND IDENTITY PROVIDER

Aruba can connect websites and digital channels to signatures, PEC, certified delivery, timestamps, digital identity, and wallet-centric flows that make transactions verifiable and legally meaningful. Through Actalis, the Group's certification authority, Aruba also issues the digital certificates that browsers, systems, and AI agents use to verify that a business is what it claims to be.

AS A EUROPEAN OPERATOR COMBINING INFRASTRUCTURE AND TRUST

Aruba offers a more coherent model for organisations that need security, compliance, and digital growth to work together as one offer, not as separate vendor layers.

CHAPTER 6

Beyond zero-click

The digital age has always moved in cycles: rapid hype, then disillusion, then a levelling out as the technology matures. The web did not eliminate physical business; mobile did not eliminate the web; and AI will not eliminate digital presence. Each cycle changes the dominant interface, redistributes value, and rewards those who rebuild their digital foundations for the next mode of interaction.

Zero-click, seen in this light, marks the start of a new model. And the next shift runs deeper than answers replacing search results: it moves from human-led browsing to AI-mediated discovery. Digital strategy is entering a post-interface era: the primary reader of a company's digital presence is increasingly an AI acting on a human's behalf, selecting, comparing, and sometimes transacting before a person ever reaches a site.

The implication is a strategic inversion. Organisations will need to make their knowledge machine-legible, their authority defensible, and their commercial functions accessible to Artificial Intelligence systems as well as to people. In that model, trust, structure, and interoperability become the deciding factors.

Over time, ambient computing and wearables may reduce screen-first browsing even further, strengthening the case for digital presence anchored in trusted identity, verified information, secure infrastructure, and transaction capability rather than in storefront-style navigation. Phone, glasses, or whatever comes next: the device matters far less than whether the brand remains discoverable, machine-readable, and trusted inside the AI layer that now sits between people and digital destinations.

The future of digital presence, in other words, is a re-architecture: from pages optimised for clicks to trusted digital systems optimised for answers, transactions, and verified identity.

A similar evolution is beginning on the personal side of digital presence as well. Italian businesses already live with digital identity through SPID and CIE; wallet-based identity under eIDAS 2.0 is the next step, and it will make verifiable, portable, and privacy-preserving trust layers central to digital interaction for individuals and organisations alike. That broader shift points toward the next frontier of digital presence: from presence on the web to presence through identity.

The next phase belongs to organisations that make their digital presence authoritative for AI, trustworthy for users, secure for regulators, and useful for real business interactions, and that keep it under their own control. Few will do it alone.

The right partner is one that enables, enhances, and empowers your digital evolution: opening up the opportunities that new technologies create, bringing decades of experience and solidity, and leaving full strategic control where it belongs, **in your hands**.

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