Breaking free from digital dependency: from audit to infrastructure

Bernard Sfez - 2026-03-23 15:50

What do you actually depend on? Which devices, servers and cloud services are outside your control, and under which jurisdiction do they operate? Do you know what your staff use beyond the officially approved tools? This third article in our series on digital sovereignty provides a practical method to audit your dependencies, assess your exposure and identify the first building blocks to reclaim.

Independent alternatives exist, they are mature and the first steps are within reach without disrupting your operations. From network hardware to servers, from hosting to cybersecurity, we detail how to lay a solid infrastructure foundation, step by step, without paralysing your activity. After storming the Bastille, you need to lay the foundations of your citadel.

In a first article, we mapped the extent of digital dependency on American technologies: from hardware to applications, through cloud and artificial intelligence, we showed where U.S. technological supremacy hides or flaunts itself. In a second article, we examined the strategies in place, the concrete advances and the contradictions that continue to hinder the reconquest of our digital sovereignty.

This third article shifts perspective. We are talking about what you can do, right now. If you are a manager or IT decision-maker, you need to act. If you are a user, you need to understand, raise awareness and facilitate the transition. Whatever the size of your organisation, this article gives you numerous keys to audit your situation, identify your room for manoeuvre and begin a progressive migration, smoothly and avoiding disruption.

The reality is clear: everyone is concerned. It is up to each of us to drive this transition, to support it, and even to demand it before entrusting sensitive information to any provider. Best practices are well established. The tools, methods and skills exist and they are mature.

And this approach is not purely defensive. Being able to demonstrate to your partners and clients that you control your data, that your hosting is sovereign and that your practices are auditable is not a cost. It is a card to play to win a contract, reassure a client or meet a compliance requirement. Digital sovereignty is becoming a competitive advantage.

Step 1: Know where you stand — the dependency audit

Before migrating anything, you need to understand precisely where you stand. No need for a five or six-figure audit to get started, but you do need a method.

Grab a sheet of paper, a spreadsheet (but not on the cloud) or create a diagram directly in Tiki Wiki which natively integrates draw.io (open source, German), without installing anything or sending data externally, and methodically list each layer of your infrastructure. For organisations with fewer than twenty workstations, this is a one-day exercise, and if you have never done it, go room by room, layer by layer. For larger ones, your IT manager probably already has part of this inventory: the challenge is to complete it with the questions that nobody ever asks.

Hardware: servers, workstations, routers, switches, firewalls, Wi-Fi access points. The goal is not to produce an inventory of serial numbers but to answer a simple question: "who manufactures this equipment, and under which jurisdiction do they operate?" As we detailed in our previous article, the new RISAA definition in the United States potentially extends the obligation to hand over data to any provider with access to equipment that transmits or stores electronic communications. This now includes network

equipment manufacturers, managed service providers, and in some cases even maintenance contractors with physical or logical access to your machines.

Operating systems: Windows, macOS, Linux? On workstations, on servers? Which versions, which licences, which renewal deadlines? This is generally the best-documented layer in organisations with a minimum of IT management. Take the opportunity to note exact version numbers: an obsolete or unsupported version is an open door to known and actively exploited vulnerabilities.

Applications: Office suite, email, video conferencing, file storage, CRM, accounting, project management... For each tool, the questions to ask are precise. Who is the publisher? Is it used locally or online, and where is the data hosted? Under which jurisdiction does the company operate? In what format can you export your data? Can your users install or use whatever they want? And above all: what do the contracts say? Is there a reversibility clause? What are the termination conditions? This contractual dimension is often neglected even though it harbours the most stubborn lock-ins. We return to this in detail further on.

Cloud services: Web hosting, backups, databases, analytics, etc. Same checklist: who operates, where, under which law? But also, concretely: where are your data and your clients' data stored right now? When you run a backup, is it on local or remote storage? Can you answer this question for every service?

Shadow IT: This is the blind spot of most organisations and often the most dangerous. Are your staff using WhatsApp to exchange internal documents? Personal Google Drive to store professional files? ChatGPT to draft business proposals containing client data? WeTransfer to send large files? A personal laptop with copies of your files? An online password manager whose hosting conditions nobody knows?

These "unofficial" practices are often the most critical and the most overlooked data leaks. And data harvesting is not limited to professional tools. The Pokémon Go affair, revealed in March 2026, is the most spectacular illustration: 30 billion geolocated images collected via players' smartphones, without most of them being aware, to build a centimetre-accurate map of the world repackaged for robotics companies. The game has since been sold to a Saudi investment fund, user data included. If a free mobile game can map the planet without its users' knowledge, imagine what the professional applications your staff install without approval are collecting.

And just days ago, a French naval officer's jogging app revealed the exact position of the aircraft carrier Charles de Gaulle in the Mediterranean. A 7 km run recorded on Strava with a public profile was enough to pinpoint a nuclear-powered warship on a classified mission. No hacking, no cyberattack, just a fitness app and a default privacy setting. The Pentagon banned connected watches on deployment back in 2018. Your organisation is probably not a military target, but the mechanism is identical: the weakest link is almost never the system, it is human behaviour.

Shadow IT is not just about applications: it covers everything your teams use thinking "it doesn't matter". Including conversations held within earshot of Siri or Alexa, whose passive listening is becoming increasingly normalised.

What the audit reveals: the same pattern everywhere

The industry and size vary. The findings rarely do. Here is what most audits reveal, whether we are talking about an SME, a local authority, a nonprofit or a school:

Documents are written in Word or Google Docs. Spreadsheets go through Excel or Google Sheets. Files are stored on OneDrive, SharePoint or Google Drive. Emails flow through Outlook or Gmail. Meetings happen on Teams or Zoom. The website uses a CDN, videos hosted on YouTube and Google Analytics to measure traffic. Accounting runs on an online platform whose ultimate hosting provider is rarely known to the client. And behind the scenes, several staff members use ChatGPT for just about anything, feeding it professional data without a second thought.

The question is not whether these tools are good. They are, and that is precisely why they dominate. The question is which jurisdiction they expose you to, and whether you are aware of it. Out of roughly fifteen everyday technology building blocks, the majority depend on companies subject to the U.S. Cloud Act. Your client data, your business proposals, your accounting, your internal communications: all of it is potentially accessible to a foreign jurisdiction. Whether you know it or not.

The contractual audit: the invisible lock-in

The technical audit is not enough. The most insidious lock-in is often contractual.

Check systematically, for every provider:

The reversibility clause. Do you have the right to export all your data in a standard, usable format? Within what timeframe? At what cost? Many cloud contracts do allow an export... in a proprietary format, making migration technically possible but practically unusable without expensive conversion tools.

Data ownership. Does the contract explicitly state that your data belongs to you? That the provider has no right to use, analyse or resell it? Watch out for "service improvement" clauses that de facto allow your data to be exploited for machine learning purposes.

Applicable jurisdiction. Which court is competent in case of a dispute? If the answer is "the State of California" or "the State of Washington", you have a problem. And if your provider is a European subsidiary of an American group, the Cloud Act still applies to

the parent company.

Termination conditions. What is the notice period? Are there penalties? Does the service continue to function during the transition period? Some contracts provide for automatic data deletion 30 days after termination, with no possibility of recovery.

Actual data protection compliance. "We are GDPR compliant" has become a marketing mantra. Demand the details: where is the data? Who has access? Does the subcontractor have subcontractors (and where are they based)? Does the DPA (Data Processing Agreement) mention transfers outside the EU? Remember: as Microsoft France's technical director acknowledged before the French Senate in June 2025, even hosting data in Europe does not guarantee immunity from American legal demands.

This work is tedious but essential. It forms the foundation of any credible exit strategy. And it often reveals unpleasant surprises that senior management prefers to ignore, until the day they no longer can.

Step 2: The replacement matrix — what to migrate, and to what

Once the audit is complete, the question becomes concrete: what do you replace each building block with? Here are the proven independent alternatives available in 2026, layer by layer, with an honest assessment of their strengths and limitations. Other solutions will emerge — the landscape is evolving fast — but these have already proven themselves in production.

Network hardware and connected devices: segment and isolate

This is the layer where pragmatism matters most. Replacing all your network equipment with European alternatives is not always possible or even necessary. On the firewall side, Stormshield (a subsidiary of Airbus CyberSecurity, R&D entirely based in France) remains to date the only firewall qualified at Standard level by ANSSI, the French National Cybersecurity Agency. The choice is therefore still limited at the high end of the spectrum, but the enforcement of the EU NIS2 directive and growing awareness of digital independence are expected to accelerate the arrival of new European offerings. For routers, MikroTik (Latvian) offers professional-grade equipment at accessible prices, and open source firmware such as OPNsense or pfSense can turn standard hardware into a powerful and auditable firewall.

For the rest — printers, cameras, meeting room screens, Wi-Fi access points, miscellaneous connected devices — replacement is not always the priority. The priority is isolation. A smart TV in a conference room does not need to be on the same network as your client files. An IP surveillance camera should not communicate with the internet without oversight. Network segmentation, meaning the separation of your equipment into watertight sub-networks according to their sensitivity level, is a simple, low-cost and remarkably effective measure. It limits propagation in case of compromise and reduces the attack surface without changing day-to-day operations.

Hosting and infrastructure: the foundation

If your servers are at AWS, Azure or Google Cloud, nothing you build on top of them is independent of U.S. jurisdiction, regardless of

the software you use.

On top of that, with these hyperscalers, the bill is an assembly of outbound bandwidth per gigabyte, API requests per unit, inter-service transfer costs and storage tiers whose logic escapes most financial departments. Many organisations discover the true cost of their cloud after just a few months of real usage. But the trap does not stop there: this pricing uncertainty continues month after month, and invoices always arrive with just enough delay for it to have become too costly to leave. Reinvesting the time, resources and money to move elsewhere? That is precisely what these providers count on to retain you.

Alternatives exist. OVHcloud and Scaleway in France, Hetzner in Germany, Infomaniak in Switzerland offer high-performance infrastructure. Their most tangible advantage is not necessarily the price per unit: it is pricing transparency. A dedicated server at a European hosting provider generally means a fixed monthly rate. For sensitive data, a growing number of providers across Europe are now certified under national security frameworks such as France's SecNumCloud or Germany's C5, ensuring immunity from extraterritorial laws.

But there is an option that many organisations overlook: the on-premise server. The quality and bandwidth available today to businesses, including professional fibre, make it perfectly feasible to host a server in-house whose cost will quickly pay for itself against ever-increasing monthly cloud subscriptions. You own the hardware, the data never leaves your premises, and you eliminate the jurisdiction question entirely. For organisations without a server room, a simple dedicated server at a European hosting provider delivers the same benefit.

Managing these servers relies on mature open source tools. Virtualmin and Webmin provide a unified interface to manage web hosting, email accounts, databases, SSL certificates and backups, all open source, licence-free and free from vendor dependency. And hardware costs have dropped considerably. A quiet, powerful server suited to an SME can be built today for under €1,500. Paid off within a few months compared to a cloud subscription, it then belongs to you for years. In this domain, digital independence is no longer a question of budget — it is a question of will.

That leaves the question everyone asks. Who manages it? Two options depending on your resources. If you have a technical profile in-house, these tools allow handling day-to-day management such as creating an email account, adding a site or checking backup status. But let us be honest. Security, system maintenance, critical update management and monitoring are skills that take time to build. This can be the starting point for a dedicated role within your organisation, supported in their upskilling by an experienced service provider. If you do not have this resource, or if you prefer to keep your teams focused on your core business, management can be fully outsourced. This is a significant part of our own work. We deploy, maintain and monitor servers for organisations that want independence without hiring a full-time system administrator.

Cybersecurity and monitoring: protecting what you have reclaimed

This is the most underestimated topic, by far. Most small and mid-sized organisations reason as follows: "We have nothing of interest, who would want to attack us?" The numbers say otherwise. According to ENISA's 2024 Threat Landscape report, SMEs are increasingly targeted precisely because they are the least protected. The IBM Cost of a Data Breach 2025 report puts the global average cost of a data breach at $4.44 million, and even for smaller organisations, the impact can be existential: studies indicate that 60% of SMEs that suffer a cyberattack close within 18 months.

You may not hold industrial secrets. But you hold names, addresses, emails, invoicing histories, supplier bank details, contractual exchanges. All of this has market value. On dark web marketplaces, a qualified client database sells, a verified email list sells, invoicing data enables wire fraud and identity theft. To give a sense of scale: the average cost per compromised personal record is estimated between $150 and $200 globally, factoring in notification costs, remediation, legal consequences and regulatory sanctions. A database of 1,000 clients that leaks represents potentially €150,000 to €200,000 in damages.

And attackers no longer spend hours or days manually preparing targeted attacks or hunting for vulnerabilities. Today, AI-powered bot farms scan, test and exploit vulnerabilities around the clock, at zero marginal cost, consuming neither time nor human resources. They cast a wide net, automatically, and the least protected organisations fall first. Ransomware does not check your turnover before encrypting your files.

The consequences extend beyond your own perimeter. Access to your data can trigger a cascade effect: it is one of your clients or partners who ends up exposed. Confidential messages containing credentials, appointments or strategic information end up in the wild. At best, your reputation takes a hit: nearly half of breached organisations report losing clients or business opportunities following an incident. At worst, insurers will seek to determine who bears responsibility for the damages, knowing that the vast majority of SMEs remain uninsured against cyber risk. And the GDPR provides for sanctions of up to 4% of annual turnover.

Reclaiming your infrastructure without protecting it is like moving into a new house and leaving the front door wide open. Independence demands rigour.

Real-time monitoring is the first line of defence. Zabbix enables continuous surveillance of your servers, services and network equipment: CPU load, disk space, service availability, suspicious connection attempts. You are alerted before the problem becomes visible to your users, and above all before an incident becomes a crisis.

Geographic access filtering is a layer of protection often overlooked yet remarkably effective. Our GeoIP cybersecurity suite, developed in-house, restricts access to your servers based on the geographic origin of connections. If your business operates in

Europe, why accept incoming connections from IP ranges on the other side of the world? Automated intrusion attempts, port scans and brute force attacks originate disproportionately from certain regions. Blocking them upstream means eliminating the noise before it even reaches your defences.

Offsite backups are the ultimate safety net. Without an external backup, a ransomware attack, a fire or a simple human error can mean permanent data loss. The baseline rule is 3-2-1: three copies of your data, on two different media, with one offsite on independent infrastructure. And above all, a backup that has never been tested in restoration is not a backup — it is a hope. Our offsite backup service runs on private infrastructure in France, with encrypted transfers, zero third-party access and documented restoration testing.

Monitoring, filtering and alerts form a coherent whole: you know at all times what is happening on your infrastructure, who is attempting to access it, and you are in a position to react immediately.

Your foundation is laid: a segmented network, a server you control, an infrastructure that is monitored and protected. What remains is to see what runs on top of it. In our next article, we will cover the application layer: email, office tools, collaboration, business management, and the thorny subject of the workstation. That is where digital independence stops being a technical matter and becomes a human one.