Email and Video Calls: Taking Back Control of Your Communications

Email and Video Calls: Taking Back Control of Your Communications

 MikaSfez - 2026-06-30 10:13

Your emails and online meetings contain most of your sensitive data: contracts, quotes, strategic discussions, and client files. They also represent your greatest point of exposure, and paradoxically, the area where regaining control delivers the highest return.

In this new installment of our series on digital sovereignty, we move from theory to practice.

The reality is clear. Every email sent through a U.S based service and every meeting hosted on a foreign platform falls under a legal jurisdiction that is not your own. Yet taking back control is far from an overwhelming task. Here's how to regain ownership of your communications, step by step, from simple actions anyone can take to solutions that genuinely keep your data under your control.

In this series, we first mapped the extent of our digital dependence, then examined what governments are doing, or failing to do, to help address it before laying the practical foundations of a sovereign digital infrastructure. In our previous installment, we left theory behind to focus on everyday practices, promising to take action one building block at a time.

This is the first building block. And it's no coincidence that we begin with communications: it's the area where the balance between effort invested and digital sovereignty regained is the most favorable. It's the best place to start because it's where you'll achieve the greatest impact in the shortest time. There's no need to overhaul everything overnight. You simply need to know where to take the first step, and then the next.

Email: Your Most Critical Digital Asset

Email is the backbone of your organization's communications. It's where contracts, customer data, strategic discussions, and password reset requests all pass through. It is also, all too often, the primary gateway for identity theft and account compromise. The diagnosis is stark, but the remedy is well within reach: email is the single most rewarding building block to reclaim. The ratio between the effort required and the digital sovereignty you regain is simply unmatched.

The First Step: Take Control of Your Domain Name

Before anything else, there is one fundamental rule: you must control your own domain name. It is the foundation of your email addresses and determines how your mail is routed. Start with the basics, your domain name and its DNS records.

If your current domain registrar is a U.S. company subject to the Cloud Act, consider transferring your domain to a European provider operating exclusively under European law. ICANN-accredited European registrars include OVHcloud, Gandi, Netim, and Scaleway in France, Infomaniak in Switzerland, and IONOS in Germany, to name some of the best-known options. The European Alternatives website also maintains an up-to-date directory of European providers across a wide range of categories.

Once your domain is secured, simply update your MX records to point to a mail server you control. The transition is seamless for your users and typically takes only a few hours to complete.

What Are the Alternatives to Microsoft 365 or Google Workspace for Email?

When it comes to the mail server itself, you don't need an overly complex setup. A Linux server running Virtualmin, a server management and web hosting control panel built on open-source technologies, provides a complete, proven email infrastructure: IMAP and SMTP accounts, spam filtering, SPF, DKIM, and DMARC authentication, SSL certificates, all hosted on a server you control yourself or with a European hosting provider. It is a robust, lightweight foundation, and one of the solutions we deploy and configure most frequently for our clients through our fully managed sovereign business email service, a genuine alternative to Microsoft 365 and Google Workspace.

On the user side, you're not locked into a particular ecosystem. Everything is built on open standards (IMAP, SMTP, CalDAV, and CardDAV), allowing you to choose whichever email client best fits your needs. Browser-based webmail solutions such as Roundcube or the webmail integrated into Tiki Wiki CMS Groupware let users access their messages from any computer. Those who prefer desktop or mobile applications can use Thunderbird, Evolution, or the native mail clients included with Windows, macOS, iOS, and Android.Everyone is free to use the interface they prefer while keeping the same emails, contacts, and calendars synchronized across all devices.

For most freelancers, SMEs, nonprofits, and public organizations, this level of infrastructure is more than sufficient. You regain control of your communications, your data remains under European jurisdiction, and you no longer depend on the policies or business decisions of a U.S. technology giant.

Going Further: When Email Becomes a Business Tool

Taking back control of your business email is already a major step forward. But for organizations that want to go further, open-source software unlocks capabilities that proprietary platforms simply cannot offer: turning email into structured business data.

This is the vision behind Cypht, an open-source webmail client that, when integrated with Tiki Wiki CMS Groupware, evolves beyond a traditional inbox into a communication management platform. The concept was presented at FOSDEM 2025, the largest European conference dedicated to free and open-source software, under the fitting title "Email as a First-Class Citizen."

This is neither an isolated nor an experimental project. It is the result of ongoing collaboration between the Tiki Wiki and Cypht development teams, with new features and improvements delivered in every release. It perfectly illustrates one of the greatest strengths of open source: software evolves through the combined efforts of multiple communities working toward a shared goal, rather than depending on the roadmap of a single vendor.

In practice, this deeper level of integration makes it possible to:

- Search across all your email accounts simultaneously without switching between multiple applications or browser tabs.
- Turn emails into structured business records. This is the feature that changes everything. An email can become a customer record in your CRM, a complaint can automatically become a support ticket, or a quotation can be attached directly to the corresponding project. Instead of remaining an unmanaged stream of messages, email becomes structured, traceable information stored on your own server and accessible only to the appropriate team.
- Migrate gradually away from Microsoft 365 or Google Workspace. Cypht is one of the few open-source webmail clients that supports Exchange Web Services (EWS) alongside IMAP and SMTP, allowing organizations to transition progressively without disrupting day-to-day operations.
- Automate message processing through configurable server-side Sieve filtering rules while integrating calendars and contacts using the CalDAV and CardDAV standards.
  Let’s be clear: this level of integration requires real thought about your processes, it’s not something you can improvise. It’s a project in its own right, one that needs to be studied on a case-by-case basis. But it highlights something essential: choosing open source isn’t about settling for a cheap substitute. Sometimes, it means gaining access to possibilities that proprietary software simply doesn’t allow.

Changing Tools Without Paralyzing Your Teams

The concern is always the same: “If I change tools, I'm going to break everything and paralyze my teams. That's a legitimate fear, and it's exactly why a successful transition is never done all at once.
Let's take a concrete example. A small organization wants to move away from an American email service. You don't switch everything over on a Monday morning. You start with what users won't even notice: securing the domain name and preparing the new server in the background with sovereign hosting. No one notices. Then you deploy the new email system on a single workstation, often someone or a small group, who's comfortable with technology, and they become a point of reference for others. Once this pilot is successful, you expand to one team, then another. Everyone moves forward at their own pace as they get used to the new tool. The two environments coexist as long as needed, with no disruption. And one day, smoothly, the transition is complete: everyone has switched over without feeling like they went through a revolution.
That's the strength of a phased migration. It connects on internal champions, respects each person's pace, and turns an intimidating project into a series of manageable steps. That's also where our support and team training make all the difference: a well-adopted sovereign tool is worth far more than one that's imposed.

Videoconferencing: The Easiest Change

A strategic meeting, a confidential interview, a client presentation, these exchanges shouldn't pass through any server you don't control. Yet every Zoom or Teams call routes your conversations, and often their transcriptions, through American infrastructure. This concern is far from marginal: the French government itself has decided to ban Teams, Zoom, and Google Meet from its services, replacing them with its own secure, sovereign open-source videoconferencing solution, which will be rolled out to its 2.5 million agents by 2027. If proof were needed, this shows that an open-source alternative to Teams and Zoom can operate reliably at scale.
What's most unsettling isn't what these platforms admit, but what they avoid promising: none clearly states the one sentence that would truly reassure you, “nothing is transcribed, nothing is stored, everything is deleted at the end of the meeting.” Instead, you're told your exchanges won't be used “without your consent,” a sentence that implicitly acknowledge data is being captured, with only a checkbox missing, one that the meeting organizer can often tick on behalf of everyone. Put simply, keep this principle in mind: what travels over public networks no longer belongs to you, and someone is already using it. We'll return to this in a future article dedicated to these astonishing terms of use.

Itsi Meet: Sovereign Video, Without Friction

The issue is the same as with email, but here the solution is strikingly simple. In fact, it's probably the most painless migration in the entire process: your users will hardly notice any difference, and resistance is virtually non-existent. Jitsi Meet replaces Zoom and Teams for video meetings: open source, encrypted, and usable without an account or installation. That doesn't mean a “bare-bones” service, however, access permissions, password-protected rooms, controlled invitations, participant moderation, everything is in place to maintain control over who joins and what is said. A simple link in a browser is all it takes, and the experience is highly optimized. You can choose sovereign hosting and install Jitsi on an internal server, or rely on a sovereign European instance, while maintaining quality comparable to proprietary solutions for meetings of up to thirty to fifty participants. You'll find all the expected features: presenter mode, screen sharing, integrated chat, hand raising, blurred backgrounds, session recording, and even live streaming if needed. Nothing is missing to establish a credible open-source alternative to Teams and Zoom.

BigBlueButton: When You Need More

For organizations with more advanced needs: BigBlueButton, originally designed for education, goes even further: shared whiteboards and collaborative annotation, breakout rooms, live polling, document sharing, and full session recording. This wealth comes at a cost: BigBlueButton is more resource-intensive on the server side than Jitsi. It's a trade-off to consider based on your actual usage, and that's exactly the kind of decision we help you make.
Here again, no data should pass through American servers. No Microsoft or Google account is required, and your external participants can join with a single click, without installing anything. It's a perfect example of the false dilemma you're so often presented with: no regaining control does not mean giving up convenience. Here, you get both.

The Weakest Link Is Almost Always Human

You can secure your servers, encrypt your communications, host your data in Europe, there will always be one vulnerability that technology alone can never fully address: human behavior. Security should never relate on the vigilance of a single individual, and yet that's often where everything is decided. We've illustrated this elsewhere with the story of the “forgotten” USB drive and the Stuxnet case: the weakest link is almost never the system itself.
And for most organizations, that weak link is often their professional email. Email remains the primary vector for the vast majority of cyberattacks, and nearly nine out of ten French companies report experiencing at least one phishing attempt each year. The scenario has become classic: an email that perfectly imitates an executive, a supplier, or a lawyer, sent at just the right moment, on the eve of a holiday or a financial closing, requesting an urgent transfer or a change in bank details. No virus, no suspicious attachment, just manipulation. And when a professional mailbox is compromised, it becomes a master key, allowing attackers to reset other accounts, intercept codes, and monitor your communications to strike at the right moment.
That's why regaining control over your communications doesn't stop at choosing the right tools. A well-configured sovereign email system already lays the right foundations: domain authentication through SPF, DKIM, and DMARC makes identity spoofing much harder, and careful monitoring helps detect unusual behavior. But technology alone is not enough. It must be paired with simple habits across your teams: be wary of urgency, verify unusual requests through another channel, never reuse your email password elsewhere, ideally relating on a sovereign password manager hosted under your control. This is precisely where employee training makes the difference, and it's a component we include in every deployment.

In Summary: Where to Start

Regaining control over your communications follows a simple logic, and that's precisely what makes it accessible. You should begin by assessing your current setup: which services you use, where your data is hosted, what falls under foreign jurisdictions, and what is truly critical to your business. From this assessment, a plan should emerge, prioritized by importance and ease of transition.
Start with what matters most, and importantly, what is least complex. First, your domain name and DNS records, the foundation of your entire professional email system. Next, your email server and clients, deployed gradually, team by team, without disruption. Then secure videoconferencing, an open-source alternative to Teams and Zoom, the most painless migration

of all. Finally, consolidate access management, so the human factor doesn't undo what technology has secured.

Each step should be autonomous, reversible, and deliver immediate value. You should move at your own pace, without ever putting everything at risk at once.

Are you wondering where to begin, and prefer to keep your internal resources focused on your core business? Don't waste time or energy—get support and reach out to our experts. Choosing open source also means supporting an open ecosystem and local expertise, rather than feeding the profits of a remote giant. This type of implementation is now common among SMEs looking to regain control over their tools.

The first step is often simpler than it seems, and the next part of this series will focus on securing your access.