STORMSHIELD

OPINION ARTICLE

IS CLOUD COMPUTING NOW SIMPLY A NON-NEGOTIABLE?

Victor Poitevin
Editorial & Digital
Manager, Stormshield

In an increasingly collaborative and interoperable world, the adoption of cloud computing continues to grow year on year. And with SaaS, IaaS, PaaS, SECaaS, SASE and many other models, cloud providers' offerings are being tailored in response to corporate technological and legal developments. Data sovereignty, latency, infrastructure security, decisions over public, hybrid or private cloud infrastructure: many questions over the value of this model need to be answered. We take a look at the main advantages and disadvantages of cloud computing, enlisting the opinions of experts along the way.

According to O'Reilly's 2021 study "*The cloud in 2021 - Adoption continues*", 90% of companies are now using cloud computing. This adoption is particularly strong in the software industry, the banking industry, retail and e-commerce, but it now seems that no one is excluded.

THE IRRESISTIBLE RISE OF THE CLOUD

According to the 2018 "*Cloud Computing Report*", 86% of respondents are concerned about security breaches and other data loss in Cloud environments. In the aftermath of the forced introduction of teleworking measures, these figures seem far from accurate: cloud services appear to have been widely adopted by companies, who are abandoning sedentary ways of working in favour of hybrid workplace/home solutions. The strong adoption of solutions such as Microsoft 365, CRM, collaborative tools, video conferencing and remote offices has provided organisations with flexibility and agility despite the health crisis.

Is it still possible to run an organisation without cloud computing in 2022? Such a scenario is hard to imagine in a world where users can now easily access online services directly from their homes - without going via multiple networks and security tools, as **Julien Paffumi,** Senior Product Manager at Stormshield, points out: "*Although using a VPN enables teleworking and mobility by providing access to company resources, it requires additional effort on the part of the user. Meanwhile, cloud platforms – whether they be CRMs or SaaS office environments – are directly available from anywhere, using any device. This accessibility makes them easier to use, and thus easier to adopt.*" This has enabled small companies without large volumes of legacy data to move their tools quickly to the cloud. This process of adoption has been facilitated by successive lockdowns since early 2020. SaaS applications can be deployed, configured and accessed from anywhere, and are just as convenient for administrators as they are for users; no more need to ask existential questions about installing software (servers and clients) or providing remote access. Not to mention the discounted pricing policies being adopted by software publishers in order to encourage companies to make the transition. But for medium and large companies, the switch is not such a simple one. Moving from an on-premises solution to a cloud solution comes at a cost, which must be planned for. Legacy data migration, user training, securing the platform and access: a project of this scale can impact employee productivity and, more generally, the company's security. A compromise solution, involving both on-premises and cloud infrastructure elements, therefore tends to be preferable.

As a logical extension of this approach, sectors that have traditionally been more closed – such as industry – are now also using cloud computing. Such shifts towards openness tend to follow a precise needs analysis, as **Vincent Nicaise**, Industrial Partnership and Ecosystem Manager at Stormshield, explains: "*Over the past five years, we have seen a measured, case-by-case adoption of cloud computing in the industrial sector. Industrial networks that had previously been autonomous can now in some cases feed back data for analysis in virtual environments.*" And for good reason, as data processing is now of central importance to corporate requirements and plans in this sector. By feeding data back into a data lake, algorithmic models provide the ability to produce predictive and prescriptive analyses. **This data feed into the cloud has enabled companies to anticipate and predict crisis situations**. This is particularly true in the case of production environments (for predicting breakdowns and supply needs, and also for optimising process continuity), in sales teams (for visualising current and future sales performance) and in security teams (for analysing and preventing cyber attacks). However, the industry sector is faced with a technical limitation: the latency inherent in cloud infrastructures. This view is shared by **Jocelyn Zindy**, Cybersecurity and Digital Transformation Sales Director at Eiffage: "*When using control applications, data processing requires millisecond precision. In this case, the cloud computing model tends to give way to edge computing, in which the processing infrastructure is located as physically close to the machine as possible, and the data is then shared in the cloud.*" This analysis is supported by figures from a January 2022 IDC study: spending on edge computing has risen by 16% in one year in Europe.

Despite the many benefits of the cloud, companies wishing to adopt it are forced to adjust their working practices. **Cloud adoption** is some way from the marketing image of a few clicks and no constraints: **it requires a multidisciplinary maturity within organisations**. But what is the cost of adoption? What requirements, and what data scope, does it cover? And most importantly, **what security rules apply?** These many issues call for strong communication between the production, logistics, marketing and commercial teams, in conjunction with the IT and security teams. Given the dominance of Big Tech in the hosting market and the introduction of the "Cloud Act", the issue of security for this data in cloud environments remains a concern for companies, especially European organisations.

THE CLOUD AND CYBERSECURITY: A MARRIAGE MADE IN HELL?

Cybersecurity and data sovereignty issues ensure that the **security of data storage in the cloud remains a major concern for organisations**. Because according to the 2022 edition of the cybersecurity barometer for companies, produced by OpinionWay and CESIN, the cloud is an environment that requires specific protection. Survey respondents rank the lack of control over the hosting provider's subcontracting chain (48%) and issues over access controls faced by the hosting provider's administrators (43%) as the two main risk factors with regard to the use of the cloud. In addition, more than 8 out of 10 CISOs surveyed still believe that providing security for data stored in the cloud is a task requiring specialist tools (86%); and specifically, tools in addition to those offered by the Cloud provider (63%).

But in this day and age, is there still any reason to be afraid of the big bad cloud? There may be more than one answer to this question. In situations where the use of a non-sovereign cloud is prohibited in sensitive environments (such as critical infrastructure operators and operators of vital importance), medium and large companies in traditional sectors are the sole arbiters of how they store their data. Information is divided into two categories: data that can be shared in the cloud and data that needs to remain in-house. According to Jocelyn Zindy, "*the cloud is used by large companies as a tool for* *decompartmentalising data. It is the place where data from different systems converges: industrial, production, infrastructure management, energy performance management and traceability systems. This environment is then subject to budgetary, performance and security constraints."* To address these challenges, cloud-based security product offerings have emerged. Sporting acronyms such as SECaaS (Security As A Service), SASE (Secure Access Service Edge) and FWaaS (Firewall As A Service), these cloud-based security solutions provide flexibility to security teams. In May 2021, Gartner announced a 41% increase in enterprise spending on cloud-based cybersecurity products – although this trend appears to be mainly a US one for the moment, with Europe remaining more cautious overall.

IS A SOVEREIGN EUROPEAN CLOUD REALLY POSSIBLE?

This caution is justified, because as soon as this data is transferred to the cloud, questions over integrity and confidentiality arise. All the more so when they are subject to questions involving the territorial scope of legislation, especially American and European. And for several years, **the European market has been feeling the need for sovereign cloud operators who are not subject to US legislation**.

Simply put, this US legislation can compel a hosting operator to provide access to customer data on request, in a regulated context. In response, in pursuit of digital sovereignty, and driven by Franco-German interests, 22 members then launched the GAIA-X project in June 2020. Originally intended as a sovereign European cloud project, the project had grown from 22 to 180 members in November of the same year, paradoxically including players such as Alibaba, Amazon, Microsoft and Google. This was something of a blow to the credibility of the project... After the (shock) departure in 2021 of two members the project is still in development but is encountering "*bureaucratic shortcomings typical of the European Union*", as reported by research firm Forrester. And this GAIA-X project is not the first of its kind: two French sovereign cloud projects were launched in 2012 with Numergy (a creation of Bull and SFR) and Cloudwatt (initiated by Orange and Thales). Unfortunately, these two projects failed to achieve commercial success: two years later, they were reporting turnovers of 6 million euros and 2 million respectively – a mere trifle compared to the billions of dollars of turnover generated by the Big Five.

In France, in 2014, the ANSSI cybersecurity agency produced a database of IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) and SaaS (*Software as a Service*) providers satisfying the agency's security recommendations, known as SecNumCloud. This certification, which underpins the promise of a trusted cloud, ensures that service providers' offerings are accompanied by a set of demanding cybersecurity standards. *"This SecNumCloud approach is an attractive one because it enables us to qualify highly demanding cloud solutions, and thus enhance confidence in French cloud players,"* Paffumi explains. *This sends a positive signal to companies. Such an approach provides a solution for adopting the cloud via trusted providers."* In line with this approach, the

3DS Outscale hosting company – a SecNumCloud-qualified player – has developed a marketplace for promoting third-party solutions with the aim of building a secure, trusted environment developed entirely in France: Simply put, a strong source of competitive value.La force des choses et les évolutions de la société semblent donc répondre à la question d'un cloud incontournable. Mais persistent les contraintes de performance, de coûts, de territorialité législative et surtout de sécurité des données qui doivent être à la base de toute réflexion des entreprises et organisations sur le sujet. Le cloud, oui, mais pas à n'importe quel prix.

Unfolding events and developments in society therefore seem to provide a clear answer to the question of whether use of the cloud is now non-negotiable. But there are still issues relating to performance, costs, legislative territoriality and – most crucially – data security, which are necessarily of central importance in any discussions by companies and organisations in this respect. The cloud, yes; but not at any price.