Digital confidence, indispensable for the cloud's success

Marc Darmon,
senior vice-president, Systèmes d'Information et de Communication Sécurisés,
&
Olivier Kermagoret,
critical systems outsourcing director, Infrastructures Critiques et Cloud

Abstract:
The cloud, a key element in the digital transition, brings competitive advantages, thus widely improving time-to-market and scalability. These conditions are indispensable to artificial intelligence, big data, the Internet of things and the DevSecOps inherent in contemporary information systems. The cloud has, in fact, been adopted: 40% of corporate information systems rely on a cloud, and the pace of growth is strong. The adoption of cloud technology must be coupled with a global strategy for making data (the new black gold) secure. There will be no "digital solution" without confidence; and no confidence, without cybersecurity. The many responses to this situation depend on the architecture's (mixed, private, public) capability of finding solutions for various classes of data and in compliance with legal requirements (as under the Cloud Act and the EU's GDPR). Technical arrangements are also necessary, such as the management of identifications in a multicloud environment, encryption, virtual architectures of security and control of the system's resilience. Managed services must also be provided for reversibility, quality and maintenance of security. This followup turns out to be the key to deploying a cloud strategy.

Within a decade, cloud computing has literally become an economic and operational reality.[1] According to a report, 40% of information systems in France have adopted a cloud architecture, a quarter of them a public version.[2] The cloud is, however, still billowing, as shown in a recent study by Thales and Pierre Audoin Consultants, which reported a growth of 33% in 2018. The various types of clouds (public, private or mixed) have now become mature enough that we can step back to examine the advantages and disadvantages when plans are made for switching to the cloud.[3]

[1] This article, including quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in April 2020.

[2] CXP GROUP (2018) "Cloud et sécurité".

[3] "Flex: le cloud de Thales, Une expérience de dix ans riche d'enseignements", https://thalesgroup-myfeed.com/LBOpenstack?elqTrackId=CC0A3828D98F78C1B431996A3BD.

The cloud, indispensable leverage for the digital transformation

Lower costs, flexibility, agility, reduced time to market… several factors underlie the cloud's success. However its major advantage is its capacity for projecting a firm toward the computerized automation of production under conditions of security (DevSecOps procedures)[4] while offering a full range of software services (SaaS: software as a service). The firm thus benefits from pooled business processes and creates value: customer relationship management (CRM), human resources (HR), shared tools and messaging services. SaaS, now the favorite way to use the cloud, accounts for 54% of the market.[5]

The cloud has thus become a major lever for the digital transformation on which a firm's competitiveness hinges. According to Bpifrance, one out of five firms will inevitably go under if they do not engage in this transformation within the next three years. The cloud is indispensable for digital applications (in particular those based on big data), the Internet of things (IoT) and artificial intelligence, all of which require highly, instantaneously scalable infrastructures. The cloud also offers the possibility of testing new applications fast with very low investments.

Cybersecurity, the "cloud confidence" factor

The cybersecurity of the cloud is a crucial prerequisite for a successful digital transformation. The statistics speak for themselves: 95% of security flaws in the cloud are related to corporate uses (in particular unsafe architectures). During the first semester 2019, 15 million attacks on connections took place, 400,000 of them successful; 85% of organizations have been specifically targeted by an attack, and 45% of them had at least one cloud account breached.[6] Using information collected by 123 million sensors that register thousands of threatening incidents per second in 157 lands, Symantec has observed the following major trends:[7]

- "Formjacking" (hijacking forms) has soared, affecting, on the average, 4800 websites per month.
- Ransomware is shifting targets from individuals to firms, where infections have increased 12%.
- More than seventy million files were stolen in poorly configured S3 compartments, a direct consequence of the rapid switch to the cloud.
- Supply chains are still easy targets, attacks on them having soared 78%.
- Connected devices are the bull's eye of cyberattacks. The IoT is a major gateway for targeted attacks, since most connected devices are vulnerable.

Unfortunately, making an information system secure is still sometimes seen as a cost, a necessary evil that has not yet proven that it can create value. Owing to the occurrence of attacks with serious effects and the growing number of regulations in the works, cybersecurity has become a

[4] "De DevOpsd à DEvSEcOps, modèles de maturité", https://thalesgroup-myfeed.com/WPDevSecOps?elqTrackId=0D7D61D30348E4D3AB2D59CF6D9.

[5] "Cloud computing: Tendances clés et perspectives 2020", http://blog.markess.com/2018/07/tendances-cloud-computing-2020/.

[6] https://www.proofpoint.com/us/threat-insight/post/cloud-attacks-prove-effective-across-industries-first-half-2019

[7] SYMANTEC (2019) "Internet security threat report", 24, 61p., available via https://docs.broadcom.com/docs-and-downloads/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf.

prerequisite for successful digital solutions. User confidence determines whether a solution will be accepted. There is no solution without this confidence, and there is no confidence without cybersecurity. Who can imagine a connected car steered from a corporate cloud but vulnerable to an attack? Cybersecurity has thus become the determinant underlying the success of the digital transformation.

We should bear in mind that information systems, henceforth massively interconnected, are permanently under attack. The more data they have and process, the more they interest hackers, whatever their motivations might be. The question is no longer whether an information system will be attacked some day, but when and how it will be attacked and how resilient it will prove to be.

Is there nothing new under the sun? Is cybersecurity in the cloud but an extension of security measures in more familiar environments? For sure, the categories of threats are the same, but the characteristics of the cloud force us to shift paradigms:

- Given the volatility of resources in the cloud, cybersecurity arrangements (*e.g.*, filtering procedures, such as firewalls) must be automatically and instantaneously rolled out.
- Users easily and rapidly subscribe to cloud services, develop and install applications; but heads of security need to keep control over their systems and have an exhaustive real-time view of the services in use.
- The attack surface is expanding, in particular when cloud services are directly accessed via public addresses.
- Responsibility for cybersecurity is shared, partly with the provider of cloud services and partly (an often larger part) with users. This distribution of responsibilities has to be brought under control.
- Using the cloud imposes specific processes and procedures that, under the cloud operator's control, are used to manage the security of data and of access (encryption, the management of identifications and keywords, etc.). It is essential for firms to appoint a trusted third party capable of helping them choose and manage these tools.
- The necessary hyperconnectivity for access to cloud services might open new points of vulnerability in interconnections and create new forms of dependency.

Multiclouds, a pragmatic approach

The market is clearly turning toward solutions involving more than a single cloud, a combination of private and public clouds. Most firms choose this strategy for two basic reasons. On the one hand, no single cloud fills all needs; and on the other hand, the choice of a single cloud would overlook the issue of the sensitivity of data (and related limitations). Pragmatism must prevail in this matter. Compromises are necessary that gauge, for each solution, the stakes and the risk/benefit ratio. There are four criteria for making a decision:

- the attractiveness of the cloud's business model,
- the attractiveness of the cloud's services (in technical and functional terms),
- the dependency on a provider, and
- the sovereignty of data.

Organizations are often preoccupied with the first two points while not realizing the risks stemming from unavailable cloud services. Although major cloud service-providers propose arrangements for seeing to the availability of applications, the applications themselves have to have been designed for these arrangements and have to be integrated in the cloud operator's "edge computing". Although public clouds have announced specifications for some services (levels of performance, availability, latency and the handling of incidents…), their commitment is actually very light since the penalties in case of a lapse of service are low or even naught, and there is no room for negotiating. The information system achitecture has to be designed with this in mind.

As for the third point, the organizations drawing their roadmap for cloud services will depend on the suppliers of these services, whence the risk of vendor lock-in. The biggest public clouds now have a catalog of high-level services — the famous, unbeatable APIs… that happen to be proprietary! These application programming interfaces awesomely accelerate new programs, but also create a dependency on the provider. Once the decision is made to use them, the possibility of reversing the decision is, given the heavy investments, more or less hypothetical. If the firm depends on parties who unilaterally modify their prices or business model, the importance and life span of the APIs and other software are decisive factors for consideration. How strategic is the software? A program for temporary use will not be negotiated like one that will be used for more than twenty years.

The fourth point, too often underestimated by naivety or overlooked, is actually the most crucial: sovereignty. Sovereignty over data refers to the control that an organization must have over its own data. Let us not forget, too, national sovereignty and the firm's sovereignty.

Handling all data alike, with an equivalent level of protection regardless of their value or sensitivity, is meaningless. A very high level of protection for all data might be counterproductive, since it does not enable the organization to benefit from all the advantages of the cloud. On the contrary, a low general level of protection will allow for far too many risks in the case of sensitive data. Data should be analyzed and classified as a function of their sensitivity when choosing cloud-based solutions and adopting the appropriate protective measures. Public clouds, owing to their abundance and the rapidity of their implementation, are attractive; but this solution might not be compatible with the sensitivity of certain sets of data.

Almost every day, masses of personal or confidential data are stolen. Data thieves in a cloud benefit from a large "scale effect". Several protective procedures can be part of a global, effective response. They are both technical and organizational: the drafting and implementation of a security policy, the adoption of good practices by those who design and develop solutions and by operatives in production, and the application of DevSecOps.[4]

Mention should also be made of the systematic encrypting of all data. Several solutions exist, such as VeraCrypt (oriented toward the needs of individuals) or Vormetrics (which Thales offers to firms). The encryption algorithm must be capable of holding up under attack: and a trusted infrastructure independent from the cloud service-provider should manage keywords. Werner Vogles, chief technology officer at AWS, stated during the AWS Summit in Berlin in February 2019, that encryption was necessary along with an independent management of encryption keys via the adoption of BYOK ("bringing your own key"). Authenticating user logins and managing user permissions have to be secure processes. Online activities have to be traced and supervised so as to detect unauthorized login attempts. Nonetheless, encrypting data is not always possible, in particular when applications (SaaS) process data. In this situation, anonymization can provide a partial solution.

On the first line of defense in cloud-related environments are the management of identifications and the control of access (as allowed by Safenet Trusted Access). Such measures for preventing intrusions are crucial, since they ensure security for all environments on the site and in the cloud (in particular logins for access to services, resources and APIs that are directly exposed on the Internet). By analyzing use cases, the targeted groups of users and the sensitivity of the applications to which users have access, *ad hoc* security policies can be implemented to appropriately manage access by balancing user friendliness with the necessary level of authentication (*e.g.*, a high level of multifactorial authentication). Managing privileged accounts has to be activated to protect administrator accounts, which are especially sensitive owing to the extent of permissions granted to them.

Finally, other important technical measures can be used to protect cloud environments, such as code audits, intrusion tests, vulnerability scans, threat detection, security supervision, etc.

The US CLOUD Act: Its impact and extraterritorial scope

The question of data sovereignty in the cloud is cogent given the additional risks stemming from acts of law with extraterritorial scope.

The report by a committee presided by Raphaël Gauvin (MP from Saône-et-Loire) on the sovereignty of France and Europe and on the protection of firms from laws and measures with extraterritorial scope opens with this worrisome remark: "*The United States of America has plunged the world into an era of judicial protectionism. Whereas the rule of law has always served as an instrument of regulation, it has now become a weapon of destruction in the economic warfare that the United States is waging against the rest of the world, including its traditional allies in Europe. […] French firms do not have effective legal tools for defending themselves against the extraterritorial legal actions brought against them.*"[8] The report establishes a nonexhaustive list of firms that are not American and have been stiffly sentenced by the United States on the grounds that their commercial practices do not fall in line with American law even though the practices in question had no direct link with the territory of the United States and these firms had complied with the law of their homelands: BNP Paribas, HSBC, Commerzbank, Crédit Agricole, Standard Chartered, ING, Bank of Tokyo, Royal Bank of Scotland, Siemens, Alstom, Télia, BAE, Total, Crédit Suisse and, perhaps tomorrow, Airbus, Areva and others.

According to the report, these investigations and sentences are deeply problematic for five basic reasons:

- They are questionable and violate the sovereignty of the countries concerned.
- The sanctions are disproportionate and menace the survival of the companies concerned.
- The investigations are conducted under the control of American prosecutors, who are directly under the executive branch of government.
- The conventions on legal assistance and rules about administrative cooperation are systematically circumvented.
- Above all, these legal actions seem to be economically motivated, the targets having been chosen on purpose.

[8] GAUVAIN R., D'URSO C., DAMAIS A. & JEMAI S. (2019) *Rétablir la sovereigneté de France et de l'Europe et protéger nos entreprises des lois and mesures à portée extraterritoriale*, report to the prime minister (Paris: Assemblée Nationale) 26 June, 102p., available via https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/06/rapport_gauvain.pdf.

The US Clarifying Lawful Overseas Use of Data Act, or CLOUD Act, seems to fit fully in with this strategy. Under certain circumstances, public cloud service-providers and network operators of American origin are legally required to provide, at the request of American judicial authorities, the data of the clients they manage or the data passing over their networks, regardless of the geographical place of storage of the data. Under this requirement, the service-provider or operator may also be forbidden to inform clients about this.

The aspects of cybersecurity discussed herein are of no help for responding to this situation. A response might be to find private or public cloud solutions offered by trusted third parties in Europe that do not fall under the CLOUD Act. For this reason, the security industry's Strategic Committee is, at the request of Bruno Le Maire, minister of the Economy and Finance, working on a set of proposals for efficient, competitive and independent cloud services in France and Europe.

From the civilian cloud to an armed forces' cloud for national defense

The shift toward the cloud in the civilian sector brings pressure to bear on national defense. But as General Crall of the US Department of Defense said, "*Can it operate successfully in an information-contested environment, when a sophisticated adversary — such as Russia or China — is jamming your transmissions and hacking your network?*" Users benefit in everyday life from the cloud, but this cloud will have to be adapted to the defense sector.

Cybersecurity in defense entails additional requirements. It is very tightly controlled with specifications, such as those used by NATO, that require a strict separation between the flow and storage of information as a function of the level of confidentiality. Related to tightened security requirements is the imperative of national sovereignty, since risks arise at the weakest link on the whole chain of security for sovereignty. A private cloud stands out as a solution for classified data and theaters of conflict. It guarantees sovereignty while providing for adaptations to conditions of use and offering the benefits of the cloud (debunkerized data, pooled resources, omni-available services) in a controlled environment.

The cloud offers an awesome degree of flexibility that deeply alters computing and thus the relations of organizations and firms with clients and customers. This deep change creates new forms of dependency that might cause an economic nightmare unless firms and administrations pursue a strategy that, by design, integrates the dimension of cybersecurity into the shifting of their activities to the cloud. The issues raised are not contradictory, and do not erect an unscalable wall: after all, solutions do exist. But a deliberate strategy is necessary for building lasting confidence and making the promise of value creation come true.