

Business
Magazine

By **Telindus**

U & S

À la une

Telindus renforce son offre multi-cloud avec AWS, Microsoft et Google

Cloud & Regulation

A possible match!

CSIOC

Sécuriser la transformation numérique

More inside

#8



MULTI-CLOUD

A NEW STANDARD AND DIGITAL TRANSFORMATION ENGINE



Between moving to the cloud and unleashing its full potential



there's a bridge.

Today, every company on the planet is looking at a new reality. One where moving to the cloud, while filled with promise, also comes with uncertainties. Eliminating those to unleash the cloud's full power requires new thinking. Security that's designed in instead of added on, so it protects every connection. The flexibility to deliver applications on-time, on any platform. And the ability to manage an entire network simply, at scale. This is Cisco SD-WAN, where the power of the network moves at the speed of the cloud.

If you can imagine it, we will build the bridge to get you there.



The bridge to possible

U&US

#8

Chers amis,

Cette 8^{ème} édition du Magazine U&US vous emmène en voyage dans LES nuages.

C'est un fait incontesté : le cloud a profondément modifié le fonctionnement des entreprises, leur apportant agilité et flexibilité mais aussi transparence et maîtrise des coûts dans un marché globalisé et en pleine mutation numérique.

Qu'il soit privé - *propre à une seule organisation* - ou public - *partagé par de nombreux clients* - le cloud se fait hybride pour offrir aux entreprises le meilleur des deux mondes. Et voilà qu'aujourd'hui il devient multiple !

Agnostique par nature, le multi-cloud renvoie à divers choix de combinaison : multiplication des abonnements dans le cloud public, diversification des applications SaaS, panachage entre cloud



public, privé et hybride. Aujourd'hui, de nombreuses organisations de toutes tailles s'appuient déjà sur des architectures multi-cloud et même les plus réticentes d'entre elles s'apprentent à sauter le pas, à l'instar du secteur financier qui a entrepris de faire cohabiter harmonieusement conformité réglementaire et technologies cloud.

Pour ces entreprises, il ne s'agit plus de savoir s'il faut adopter LE cloud, mais d'apprendre à tirer parti de l'immense potentiel DES clouds, condition nécessaire à une transformation numérique réussie.

Ce numéro spécial "clouds" vous donne les clés d'un nouveau modèle où la combinaison de services multi-fournisseurs IaaS, PaaS, SaaS, publics, privés ou hybrides permet aux organisations de sélectionner l'offre adéquate pour chaque besoin. Je vous laisse donc découvrir sans plus attendre cette nouvelle édition qui ouvre notamment ses colonnes à deux géants de l'industrie numérique.

En vous souhaitant une excellente lecture.

GÉRARD HOFFMANN
CEO, Proximus Luxembourg

SOM- MAIRE

- 5** À la une
- 8** Cloud computing
Towards enterprise wide implementation
- 18** Timeline
- 20** Multi-cloud
Une approche portée par les priorités métier
- 28** Key Figures
- 32** Cloud & Regulation
A possible match!
- 52** Case study KNEIP
KNEIP entrusts the protection of their data to Telindus
- 56** Cyber Security & Intelligence Operations Center
Sécuriser la transformation numérique
- 62** Afterword

U&US #8 Avril 2019

PROXIMUS LUXEMBOURG S.A.
18, rue du Puits Romain
Z.A. Bourmicht 8070 Bertrange
Tél : +352 450 915-1

GESTION ÉDITORIALE
Michaël Renotte

PHOTOGRAPHIES
Loris Romano & Olivier Dessy

CONCEPTION GRAPHIQUE
Deuux

IMPRESSION
1000 exemplaires

POUR ÉCRIRE À LA RÉDACTION
marketing@telindus.lu

 @telindustelecom

 /Telindus-luxembourg

À LA UNE

La certification au cœur de la stratégie de Telindus

Trois ans après l'obtention de sa certification ISO 27001, Telindus vient d'être recertifié par Bureau Veritas avec un élargissement du périmètre aux services de cybersécurité.

Ainsi le système de management de la sécurité de l'information soutenant les activités d'approvisionnement, d'exploitation et de supervision opérationnelle de cloud, des services de cyber-sécurité, des services managés et des services d'externalisation fournis par Telindus S.A. à ses clients est conforme aux attentes de cette norme.

Cette certification vient reconnaître officiellement à nouveau nos qualités opérationnelles de managed cloud services provider. Notre demande d'extension du périmètre vers la cybersécurité est une démarche naturelle: nos clients ont

besoin d'un partenaire de confiance pour l'externalisation de leur IT, supportant leurs activités stratégiques, les aidant à s'adapter aux changements réglementaires et les protégeant des risques de plus en plus élevés de cyberattaques. Nous leur démontrons ici que la sécurité est intégrée et managée by-design et by-default par nos équipes selon une approche fondée sur les risques.



Cloud et Réglementation : la rencontre possible grâce à un partenariat étroit avec Google et Cisco

Comment le cloud public peut-il apporter de la valeur à l'industrie financière ?

La réponse est sans ambiguïté : informatique sans serveur, extension des ressources à la demande, Intelligence Artificielle prête à l'emploi et Apprentissage Machine sont autant de vecteurs de croissance offerts par le cloud au secteur financier.

Telindus a pour ambition de faciliter et d'accélérer l'accès des institutions financières au cloud public en

combinant la valeur du cloud public avec les capacités de ses propres structures d'hébergement. Pour y parvenir, la société coopère étroitement avec Cisco, partenaire de longue date et leader dans le domaine de la connectivité et des réseaux, et avec Google qui a construit sa plateforme cloud sur base d'une approche résolument open source.



Telindus, un consultant partenaire d'Amazon Web Services

Avec ses ingénieurs certifiés, Telindus permet aux entreprises de trouver la configuration idéale sur ce cloud public de première classe. Telindus est aussi en mesure de fournir des ressources AWS, de les intégrer et de les exploiter.



Telindus renforce son cloud hybride et déploie la solution Microsoft Azure Stack avec Hewlett Packard Enterprise

Telindus, hébergée au Luxembourg, propose une plateforme de cloud agile et flexible basée sur les technologies Microsoft Azure Stack et les équipements HPE.

Les fonctionnalités de développement uniformes et de déploiement universelles d'Azure Stack, associées à l'expérience acquise par Telindus, répondent aux exigences spécifiques des entreprises, quel que soit leur secteur d'activité. Azure Stack est

disponible "as-a-service" depuis les centres de données de Telindus.

Telindus permet aux entreprises de bénéficier de l'agilité et de l'évolutivité du cloud public avec une vraie "expérience Azure", tout en offrant des niveaux de contrôle et de performance équivalents à ceux d'un centre de données local hautement sécurisé.



Telindus et Resultance partenaires pour une transformation numérique réussie

Telindus et le cabinet de conseil en performance opérationnelle Resultance partagent la conviction qu'une transformation numérique réussie doit s'appuyer sur une réflexion et une analyse de création de valeur. Les entreprises doivent tirer profit des technologies de l'information et de la communication afin de gagner en compétitivité, en performance et renforcer leur capacité à innover. Il s'agit d'amener la technologie là où elle créera le plus de valeur pour l'entreprise.



C'est donc tout naturellement que Telindus et Resultance ont choisi d'unir leurs forces pour aider les entreprises à réussir leur transformation digitale, en alliant l'expertise technologique de Telindus au savoir-faire métier de Resultance.

Les partenaires œuvrent dans le cadre de plusieurs programmes dont Fit4Innovation ou encore Industrie 4.0 et comptent déjà à leur actif plusieurs projets ambitieux au Luxembourg.

Telindus et Agile Partner unissent leurs forces au service de la transformation digitale de leurs clients

C'est en écoutant les besoins exprimés par les entreprises qu'Agile Partner et Telindus ont décidé de concrétiser leur ambition de partenariat. Les deux sociétés complètent ainsi leurs offres cloud et proposent désormais un accompagnement de bout-en-bout, couvrant tant la sphère applicative, que l'infrastructure et la consultance.

Ensemble, ils accompagnent les entreprises luxembourgeoises de toute taille dans leur voyage vers le cloud à tous les niveaux: stratégie, gestion du changement, conduite de projet, logiciel et infrastructure.



Présent sur le marché luxembourgeois depuis 15 ans, Agile Partner est un expert reconnu dans la transformation des applicatifs.

Telindus apporte le conseil en architecture hybride, les services de migration et de gestion en environnement multi-cloud.

Ensemble, Agile Partner et Telindus possèdent tous les atouts pour devenir les partenaires de référence des entreprises confrontées à un défi de transformation stratégique. Ce partenariat permet aux clients de mieux appréhender l'ensemble des défis posés par la transformation digitale en accompagnant au mieux leur migration vers le cloud.

CLOUD COMPUTING

**TOWARDS
ENTERPRISE WIDE
IMPLEMENTATION**

10 years ago, cloud computing began to spread as a buzzword for server virtualization. At that time, sticking a "cloud label" onto anything that looked like shared hosting, colocation, or other service-based IT solutions allowed vendors to advertise old products as fresh innovations. This created a lot of confusion around the technology, and it wasn't until 2010, when Gartner issued the first Magic Quadrant dedicated to IaaS, that the skies finally started to clear for cloud computing.

Today, a decade later, the cloud has evolved into an essential business technology. Virtually all organizations, regardless of size, industry, or location, now rely on the cloud for a broad range of business needs, from SaaS-based versions of legacy applications to IaaS-deployed strategic enterprise-level systems.

This evolution has largely been driven by the uninterrupted development of use cases for cloud computing beyond cost reductions and productivity gains. Practically all the major IT innovations in the recent years – such as the Blockchain, AI, Machine Learning, Big Data or Advanced Analytics – owe much of their existence to the cloud.

In this article, we offer you an overview of the current state of cloud computing, from overall trends to adoption rates and developments for specific industries, a glance back into the history, as well as a look ahead into the future.

A fast growing industry

Strong updrafts

Although findings about the volume and growth rate of the global cloud computing market vary from one research firm to another, they all indicate that **the cloud continues to grow at a faster pace.**

Gartner forecasts that by the end of 2019, total worldwide revenues from public cloud computing will grow by 17.3% from the previous year's figure to €181.83 billion, up from €155.03 billion in 2018¹. For its part, Forrester predicts that the global cloud computing market will exceed €176 billion in 2019, expanding at more than 20%². On a longer-term basis, Gartner sees cloud computing's market size growing to over €224 billion by 2020³, while Forrester estimates that the Public Cloud will reach €204 billion in 2020⁴. IDC places this figure at €328 billion two years later, in 2022⁵.

Cloud Wars

A handful of hyperscale players controls a large portion of the different public cloud segments. These giants have dominated the cloud for several years now and are still expanding at impressive rates at the expense of non-cloud IT companies and other smaller cloud providers. According to Forrester, **Amazon**, **Microsoft**, and **Google** will have captured 76% of the cloud platform market by the end of 2018, a share that should grow to 80% in 2020⁶.

IBM and **Alibaba** are also firmly engaged in the battle, fighting for the fourth place in the ranking of the world's biggest public cloud providers. In cloud computing, Alibaba is primarily known for its rapid growth in China, where the company has long been the leading player in e-commerce. But the Chinese giant is no longer just a regional power. According to Synergy Research Group, Alibaba surpassed IBM in the first quarter of 2018 to become the world's fourth biggest provider of cloud infrastructure and related services⁷.

¹ Gartner, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019

² Forrester, Predictions 2019: Cloud Computing

³ Gartner, op. cit.

⁴ Forrester, Public Cloud Market Will Grow To \$236 Billion In 2020

⁵ IDC, Worldwide Public Cloud Services Spending Forecast to Reach \$210 Billion This Year

⁶ Forbes, Forrester's 10 Cloud Computing Predictions For 2018

⁷ Synergy Research Group, AWS is Leading the Public Cloud Market in all Major Regions

Cloud adoption and usage

Winds of change

The cloud is seeing increased usage and adoption rates among businesses considered as a whole. But the numbers vary according to business size, cloud architecture (public, private, hybrid) and cloud segment. The 2018 edition of Right Scale's State of the Cloud Report shows some very revealing cloud adoption and usage trends ⁸:

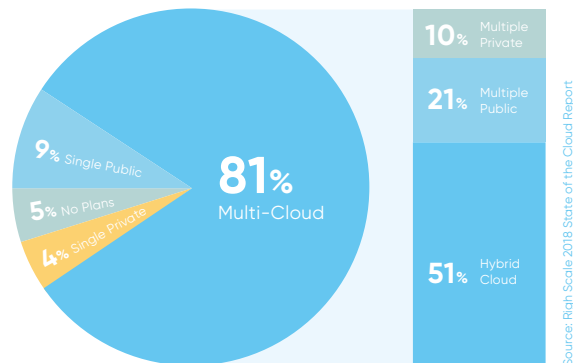
- 81% of enterprises have a **multi-cloud strategy** (RightScale's definition of multi-cloud is a combination of public and/or private cloud architectures, see Fig. p 11)
- Cloud users are running applications in an average of 2.7 public clouds and 3 private clouds
- Both **public and private cloud adoption grows**. However, many more enterprises see public cloud as their top priority, up from 29 percent in 2017 to 38 percent in 2018
- **SMB companies** run 80% of workloads in the cloud (48% in public cloud and 32% in private cloud)
- **Large companies** run 77% of workloads in the cloud (32% in public cloud and 45% in private cloud)
- **Barriers** to cloud adoption (expertise, security, budget, etc.) are lessening
- Top cloud challenges are **security and spend**

⁸ RightScale, State of the Cloud Report 2018



Respondents with 1,000+ Employees

81% of companies have a multi-cloud strategy



“As it enters its second decade, cloud computing is increasingly becoming a vehicle for next-generation digital business, as well as for agile, scalable and elastic solutions.”

DAVID MITCHELL SMITH

Vice President and Gartner Fellow in Gartner Research

“By 2021, more than half of global enterprises already using cloud today will adopt an all-in cloud strategy.”

GARTNER,

"Predicts 2017: Cloud Computing Enters its Second Decade"

Types of cloud deployments

There are different ways to deploy cloud resources. Options for deployment include public, private, and hybrid cloud. All three scenarios provide similar benefits, including cost-effectiveness, performance, reliability, and scale, but which deployment method you choose depends on your business needs.

Public cloud

Public clouds are owned and operated by a third-party cloud service provider and deliver their computing resources like servers and storage over the Internet. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud “tenants”. Public cloud deployments are frequently used to provide web-based email, online office applications, storage, and testing and development environments.

Private cloud

A private cloud consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization's on-site datacenter, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network and the hardware and software are dedicated solely to your organization. Private clouds are often used by organizations with business-critical operations seeking enhanced control over their environment.

Hybrid cloud

Hybrid clouds combine public and private clouds, bound together by technology that allows data and applications to be shared between them. By allowing data and applications to move between private and public clouds, hybrid cloud gives businesses greater flexibility and more deployment options. For instance, you can use the public cloud for high-volume, lower-security needs such as web-based email, and the private cloud – or other on-premises infrastructure – for sensitive, business-critical operations like financial reporting.

Types of cloud services

Most cloud computing services fall into three broad categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). These are sometimes called the cloud computing stack, because they build on top of one another.

SaaS

is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure, and handle any maintenance, like software upgrades and security patching. Users connect to the application over the Internet, usually with a web browser on their phone, tablet, or PC. Common examples are email, calendaring, and office tools.

IaaS

is the most basic category of cloud computing services. With IaaS, you rent IT infrastructure – servers and virtual machines (VMs), storage, networks, operating systems – from a cloud provider on a pay-as-you-go basis.

PaaS

refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development.

Sectorial focus

While the cloud transforms every single sector in the global economy, here we simply focus on the financial services, healthcare, and manufacturing verticals. The reason being that these three sectors are among the industries which will be massively impacted by the cloud, according to an Economist Intelligence Unit study⁹.

Financial services

In a heavily-regulated industry like the financial services sector, compliance is a huge factor that determines how quickly firms in the sector adopt new technologies like the cloud. With highly sensitive data involved, security and privacy also rank high on the list of barriers to implementation.

Increasingly, however, as cloud providers tailor their offerings to meet the industry's needs, many financial services firms are moving their applications to the public cloud. In that respect, a number of developments have helped increase cloud adoption and usage in the financial services industry¹⁰:

- Improved data security and privacy capabilities
- Narrowing gaps in skills and expertise
- Lesser apprehensions about vendor lock-in
- Willingness to reengineer internal processes and workflows

As a result, two key trends now shape how the cloud impacts this sector. The first is the adoption of cloud-based applications for back office and customer-facing internal systems. The second is the emergence of FinTech solutions that provide cloud-enabled applications and software for delivery of financial services.

Healthcare

Similarly, the healthcare sector has been slow to adopt cloud technology because of serious compliance concerns and data security issues. For some time after other industries started effectively moving to the public cloud, healthcare's cloud adoption rates remained among the lowest.

But the attitude of healthcare organizations toward the public cloud has evolved significantly, as cloud providers have introduced tools and measures like end-to-end data encryption, access management services, and personal data and health information protection mechanisms.

Globally, the sector is projected to see double-digit growth in cloud spending, which is expected to reach €30 billion by 2022. The European market for healthcare cloud computing should reach €7.4 billion by 2022, growing at a rate of 12.4% during the period from 2017 to 2022¹¹.

⁹ The Economist Intelligence Unit, *Ascending cloud: The adoption of cloud computing in five industries*

¹⁰ The Wall Street Journal, *Deloitte Insights, Cloud Adoption in Financial Services*

¹¹ ReportLinker, *Healthcare Cloud Computing: Global Markets to 2022*

The Economist Intelligence Unit study outlines a few cloud computing use cases in the healthcare industry as follows ¹²:

- Remote diagnostics and treatments
- Supporting preventive care
- Improving treatment outcomes
- Point-of-care access to medical data
- Development of mobile and IoT ecosystems

Manufacturing

Cloud computing has also been slow to take off in the manufacturing industry. This is largely due to the intrinsic complexity of manufacturing processes and the difficulty to embed cloud computing into physical systems. This kept switching costs and barriers to adoption very high for most manufacturers so that moving away from legacy IT systems was not a viable option ¹³.

Today, however, manufacturers are heavily investing in cloud-based IT platforms like IoT integration, greatly expanding the industry's cloud adoption and usage. An IDC survey of manufacturing firms reveals a clear uptrend in the industry's reliance on cloud computing ¹⁴:

- 66% of respondents use a public cloud implementation of 2 or more applications, while 68% use a private cloud
- Respondents also plan to increase the cloud's share in their annual IT budget
- Cloud-based services will make up almost 50% of organization-level software usage among manufacturers by 2023

The Economist Intelligence Unit also reveals several key areas where the cloud plays a big role in manufacturing: production processes, supply chain management, design and prototyping, as well as inventory, order and distribution management ¹⁵.

¹² The Economist Intelligence Unit, op. cit.

¹³ The Economist Intelligence Unit, op. cit.

¹⁴ IDC, *Cloud Adoption in the Manufacturing Industry*

¹⁵ The Economist Intelligence Unit, op. cit.

3 innovations that will reshape the cloud

AI-enabled Enterprise IoT

As the number of enterprise IoT (Internet of Things) projects double and IoT standardization and interoperability initiatives start taking root, it seems that the technology has finally come of age. According to the IoT expert community RT Insights, enterprises now leverage IoT capabilities to generate measurable business value rather than simply using IoT as a means for connecting devices ¹⁶.

AI (Artificial Intelligence) enables much of this transformation. When embedded into IoT systems, AI and Machine Learning become the brain while IoT provides ways to both gather data and to act on AI system's decisions. This synergy is already being used in manufacturing for predictive analytics, in healthcare for remote patient monitoring, and in other industries.

Serverless architectures

Serverless computing became a focus of attention for the developer community in 2014 when Amazon launched AWS Lambda as a cloud service to help developers concentrate on the application at the task level, without worrying about managing server-level resources or processes.

Serverless is now one of the most interesting trends in cloud computing. Going serverless means that developers simply have to run their code via hosting providers like Amazon, Microsoft, Google, etc. These vendors, in turn, manage application runtimes – load balancing, server provisioning, OS infrastructure, etc. – and deliver the resources needed by the application on a pay-as-you-go basis.

Edge and fog computing

Edge and fog computing are ways to efficiently manage the massive amounts of data generated by IoT devices. These two related architectures minimize latency in the cloud by carrying out much of the critical data processing close to where the data comes from – sensors, relays, and other connected devices – rather than doing all the computing at traditional cloud data centers.

While the two terms are often used interchangeably, there is actually a major difference between the two architectures. In edge computing, data processing takes place directly inside connected devices, like programmable automation controllers. Fog architectures, on the other hand, move computing to the local area network level, such as fog node or IoT gateway.

IDC predicts that by 2019, 45% of IoT-created data will be stored, processed, analyzed, and acted upon close to, or at the edge of the network ¹⁷. The research firm also forecasts that infrastructure managers will be asked to deliver solutions that reduce time-to-value from data collected from connected devices, beyond the four walls

¹⁶ RTInsights.com

¹⁷ IDC, IDC FutureScape: Worldwide Internet of Things 2016 Predictions

¹⁸ IDC, IDC FutureScape: Worldwide IoT 2018 Predictions

of the datacenter. Therefore, by 2020, IT spend on Edge Infrastructure will reach up to 18% of the total spend on IoT infrastructure, driven by deployments of open and converged software-defined IT/OT systems¹⁸.

Industries like manufacturing, financial services, healthcare, and telecom are already seeing the benefits of faster, near-real-time, and continuous data processing from connected devices.

“ By 2025, 80% of enterprises will have shut down their traditional datacenter. ”

Gartner Blog Network,

The data Center is Dead, David Cappuccio

TIME LINE

After a long history, public cloud computing comes to Luxembourg

Cloud Computing is not a twenty-first century technology. Cloud computing developed gradually through a number of milestones which include Grid Computing, Utility Computing, Application Service Provision, and Software as a Service. But the overall concept of delivering computing resources through a global network has started in the sixties.

1969 ARPAnet

The Advanced Research Project Administration (ARPA) is established by the US government. Its initial purpose was to communicate and share computer resources among scientific users.

Early 1980s TCIP/IP

The National Science Foundation (NSF) launches an initiative to build a national backbone network based on TCIP/IP protocol and link supercomputer centers and regional academic networks.

1986 NSFNET project

The NSF creates network access to the supercomputer sites in the US.

Late 1980s

Commercial Internet Service Providers (ISPs) begin to emerge.

1990 The rise of the Internet

The Internet becomes visible to all when computer scientist Tim Berners-Lee invents the World Wide Web. In doing so, Berners-Lee links hypertext documents to an information system, making it accessible from any node on the network.

1998 Virtualization

VMware Inc. introduces the concept of virtualization on the x86 platform.

1999 Salesforce.com

A pioneer in delivering enterprise applications via the cloud, now known as Software-as-a-Service (SaaS). Salesforce multi-tenant applications are designed to run in the cloud, be accessible over the internet and be used by large numbers of customers at low cost.

2002 Amazon Web Services

Shortly after the launch of Salesforce, Amazon launches its Amazon Web Services (AWS) platform with the aim of delivering a suite of cloud-based computing services to customers that would only pay for what they use.

2006 Amazon Elastic Compute cloud

Amazon launches its Elastic Compute cloud (EC2), a commercial web service allowing small companies and individuals to rent computers to run their own applications on.

2008 Google App Engine

Google launches its Google App Engine Platform-as-a-Service, allowing developers to host web applications in its managed datacenters.

2008 Gartner begins to talk of cloud

Research firm Gartner begins to discuss the rise of cloud computing, describing cloud computing as "a style of computing in which massively scalable IT-related capabilities are provided as a service using internet technologies to multiple external customers."

2010 Microsoft Azure

Software giant Microsoft enters the cloud market with the launch of its cloud computing platform Azure in 2010, after it was announced in 2008.

2010 Rackspace OpenStack

Rackspace and NASA pioneered a free open source software platform for cloud computing - OpenStack - to help organizations run cloud computing on standard hardware. Since 2016, OpenStack has been managed by the OpenStack Foundation, a non-profit entity established in 2012. Over 500 companies have joined the project since.

2011 IBM SmartCloud

IBM launches SmartCloud, a line of enterprise-class cloud computing technologies for building private, public and hybrid clouds.

2013 Google Compute Engine

Google Compute Engine is officially launched in 2013 as an addition to the Google Cloud Platform. The offering stands as the IaaS component of the platform.

2017 CSSF Cloud Circular

On May 17 2017, the CSSF publishes the circular 17/654, with the purpose to clarify the regulatory framework governing IT outsourcing in Luxembourg relying on a cloud computing infrastructure provided by an external provider.

MULTI CLOUD

**UNE APPROCHE
PORTÉE PAR
LES PRIORITÉS
MÉTIER**

L'opportunité d'exploiter les avantages propres à chaque fournisseur de services cloud apparaît aujourd'hui comme un élément moteur du développement des entreprises. L'approche multi-cloud est ainsi en passe de devenir une stratégie de choix pour les organisations qui cherchent à accélérer leur transformation numérique.

Le multi-cloud – le fait de déployer les applications ou de répartir les ressources sur plusieurs plateformes de cloud public – est sans aucun doute l'un des sujets de réflexion prioritaires de la plupart des décideurs informatiques. Soucieuses de ne pas se laisser enchaîner à une solution cloud unique, les entreprises décident de plus en plus souvent de combiner différentes solutions cloud plutôt que de faire le choix d'un seul fournisseur parmi l'ensemble des offres disponibles.

L'adoption du multi-cloud par les entreprises devrait connaître une forte croissance au cours des prochains semestres. Gartner prévoit ainsi que le multi-cloud constituera la stratégie commune de 70% des entreprises d'ici la fin de l'année 2019¹. Une étude menée par Forrester à l'échelle mondiale révèle pour sa part que 86% des entreprises utilisent plus d'un fournisseur de cloud dans le cadre de leurs efforts de transformation numérique². Et en observant l'année dernière que 40% des organisations européennes avaient étendu leurs applications au cloud, IDC soulignait déjà l'urgence de la nécessité d'une stratégie multi-cloud pour les entreprises³.

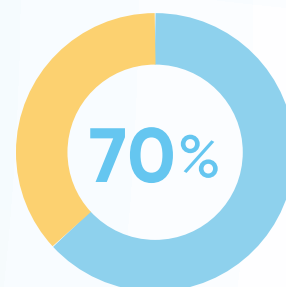
Les apports du multi-cloud

La clé du succès d'une stratégie multi-cloud réside dans une bonne compréhension de ce que chaque cloud peut apporter à l'entreprise afin de tirer parti des avantages respectifs de chaque fournisseur. La mise en œuvre d'une telle stratégie apporte un large éventail d'avantages aux organisations. Le multi-cloud offre notamment à chaque département la flexibilité de sélectionner un service parfaitement adapté à ses besoins, au lieu d'être contraint par une structure unique et commune à toute l'entreprise.

Plus largement, en multipliant les plateformes cloud, les entreprises évitent d'être liées à un seul fournisseur, situation susceptible de les exposer à des hausses de prix inopinées et à des changements substantiels dans la nature ou le niveau des services reçus.

En diversifiant leurs investissements entre plusieurs fournisseurs de cloud, les entreprises ont également davantage de choix quant à l'endroit où elles exécutent leurs charges de travail, ce qui leur permet d'en gérer plus efficacement les coûts.

L'adoption d'une stratégie multi-cloud apporte en outre une plus grande flexibilité géographique dans la gestion des données. Les principaux fournisseurs de cloud possèdent des centres de données partout dans le monde,



of enterprises will be implementing a multi-cloud strategy by 2019

Gartner

mais certaines entreprises peuvent néanmoins exiger que les données relatives à des charges de travail spécifiques soient stockées à l'intérieur de certaines frontières. Le multi-cloud permet aux entreprises de trouver facilement une réponse à ce type de besoin, tout en bénéficiant des avantages d'une plateforme cloud mondiale. Les entreprises peuvent également escompter une réduction des risques de perte généralisée de données ou d'indisponibilité des applications en raison d'une défaillance locale.

¹ Gartner, David J. Cappuccio, *The Future of the Data Center in the Cloud Era*

² Forrester Consulting, *Multi-cloud Arises from Changing Cloud Priorities*

³ IDC, Giorgio Nebuloni, *40% of European Organizations Already Stretch Applications Across Clouds; Multi-cloud Strategy Urgently Needed*

Multi-cloud et sécurité

Avec l'entrée en vigueur, il y a quelques mois, du nouveau règlement européen sur la protection des données (GDPR) et les failles de sécurité à grande échelle qui font régulièrement la une des médias, la sécurité des données demeure au centre des préoccupations des décideurs informatiques.

Alors que l'approche multi-cloud rencontre un succès croissant, de nouvelles technologies, comme l'informatique sans serveur (serverless computing), la conteneurisation et l'apprentissage machine (machine learning), gagnent elles aussi en popularité grâce aux avantages de sécurité qu'elles apportent au cloud.

L'informatique sans serveur, par exemple, permet aux instances cloud des mises à l'échelle instantanées et des applications de correctifs immédiates, réduisant ainsi les cyber-risques. L'apprentissage machine, quant à lui, peut aider les serveurs à identifier les modèles de comportements malveillants et à y réagir plus rapidement que ne le peut un intervenant humain.

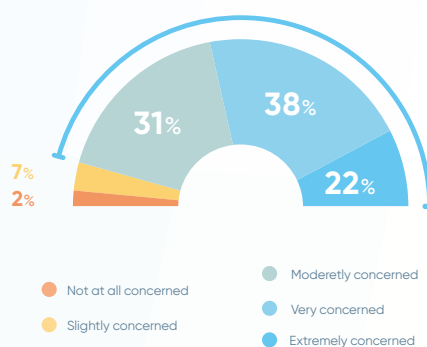
Si elle est conçue à cette fin, une stratégie multi-cloud peut grandement contribuer à prévenir les pertes de données massives en cas de brèche, les informations étant réparties sur plusieurs plateformes différentes.

Les principales caractéristiques d'un déploiement multi-cloud couronné de succès résident dans une étroite intégration et des modes opératoires cohérents. Les entreprises doivent prendre en compte le fait qu'une solution de sécurité unique ne peut pas couvrir tous les cas de figure, ce qui nécessite un effort supplémentaire en matière de sécurité et de gouvernance. L'adoption du multi-cloud continuant à gagner en popularité, il deviendra de plus en plus crucial d'être à même de surveiller et de contrôler toutes les couches de données.

Cloud Security Concerns on the Rise

While adoption for public cloud computing continues to surge, security concerns are showing no signs of abating. An overwhelming majority of cybersecurity professionals (91 percent) say they are extremely to moderately concerned about public cloud security, up **11 percentage points from last year**.

91% Organizations are concerned about cloud security



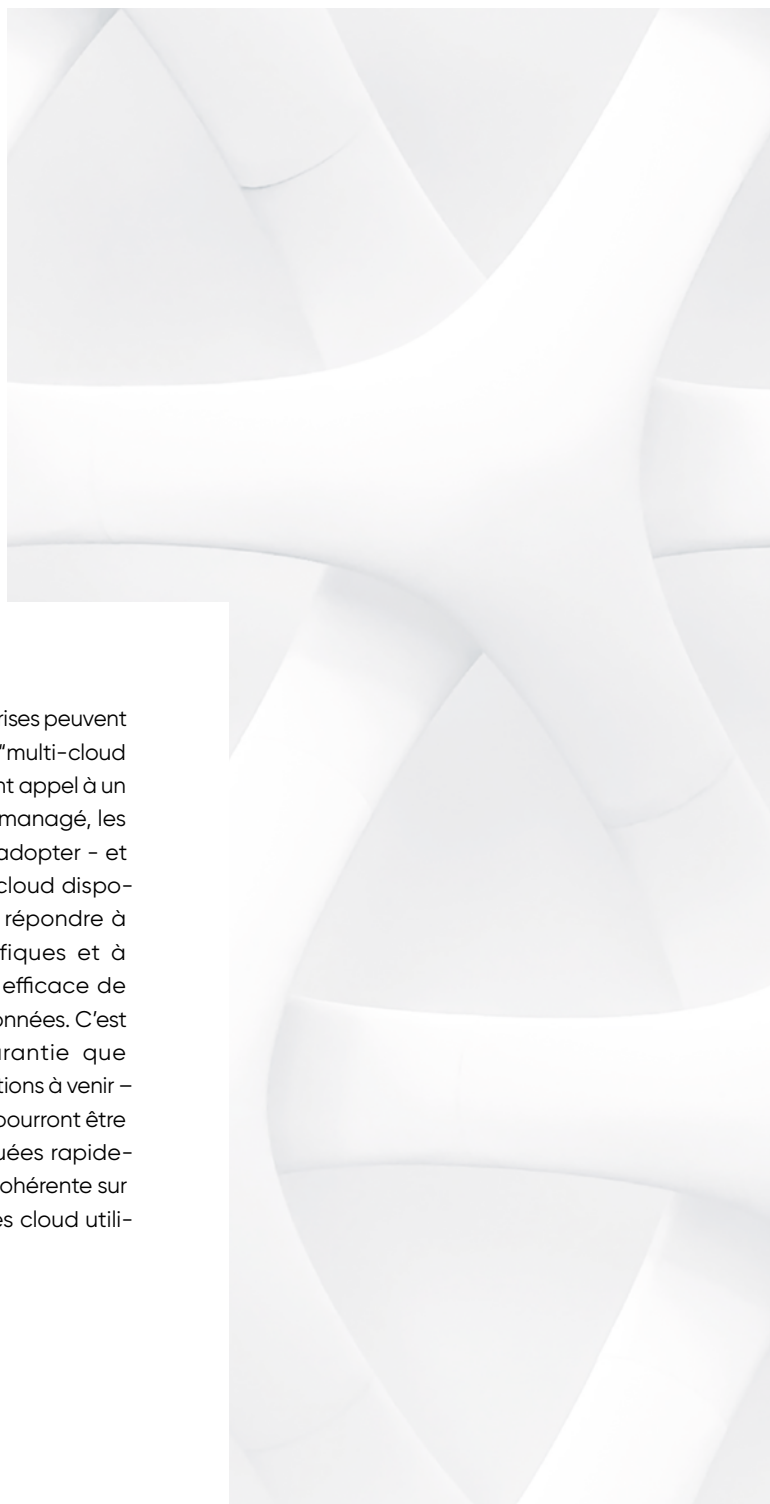
Source: Cybersecurity Insiders, 2018 Cloud Security Report

Faire d'une stratégie multi-cloud une réalité pour les entreprises

Même si les avantages du multi-cloud sont évidents, les entreprises risquent de connaître des incidents de sécurité si elles ne parviennent pas à gérer efficacement les données lorsqu'elles se déplacent entre les différents clouds, ou à tenir compte du fait que chaque cloud peut répondre à ses propres normes de sécurité.

Au vu du développement rapide du secteur du cloud et de la pénurie de main d'œuvre disposant des compétences en la matière, il est impératif que les entreprises se tournent vers des partenaires pour garantir un fonctionnement optimal de leurs systèmes d'information.

C'est là que les entreprises peuvent envisager l'option du "multi-cloud as a Service". En faisant appel à un fournisseur de cloud managé, les entreprises peuvent adopter – et adapter – les offres cloud disponibles de manière à répondre à leurs besoins spécifiques et à assurer une gestion efficace de la sécurité de leurs données. C'est également une garantie que toutes les réglementations à venir – mêmes complexes – pourront être assimilées et appliquées rapidement et de manière cohérente sur toutes les plateformes cloud utilisées par l'entreprise.



Cloud Benefits vs. Expectations

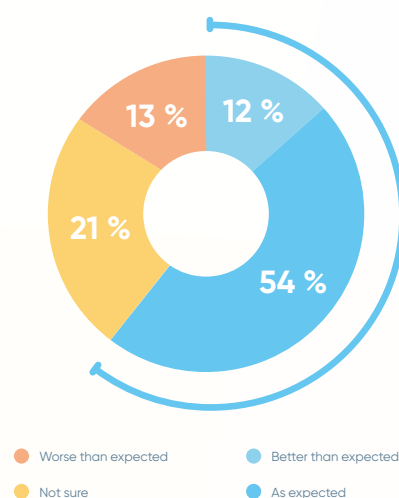
How does the reality of cloud computing hold up against the promise of reduced cost, increased agility, accelerated time-to-market or improved uptime? Sixty-six percent of the IT professionals surveyed said their cloud investments are meeting or exceeding expectations. Notably, about one out of five respondents (21 percent) were unsure if the cloud had delivered on the promised benefits to the organization.

À mesure que le cloud s'affirme comme la nouvelle norme et que l'adoption du multi-cloud continue de progresser, les décideurs informatiques doivent définir une stratégie claire quant à la manière d'intégrer ces solutions dans leurs activités.

Il est essentiel que cette stratégie soit pensée dès le départ de manière à pouvoir évoluer au fil du temps et mise en œuvre de façon à provoquer le moins de perturbations possible. En agissant de la sorte, les entreprises disposeront des outils nécessaires pour construire des infrastructures qui leur permettront de rester en phase avec les innovations technologiques et de développer leurs avantages concurrentiels.

66%

Think their cloud investments are meeting or exceeding expectations



Multi-cloud et cloud hybride

Si le multi-cloud et le cloud hybride présentent certaines similarités, il s'agit toutefois de modèles différents.

Le cloud hybride correspond à une architecture de cloud computing qui utilise à la fois un cloud privé local et un cloud public tiers, ainsi qu'une orchestration entre les deux environnements. Souvent, une entreprise adopte le cloud hybride pour rencontrer un besoin spécifique, telle que la possibilité d'exécuter des charges de travail en interne et de les porter par la suite dans le cloud public, lorsque les demandes de calcul augmentent.

Le modèle multi-cloud fait communément référence au recours à plusieurs fournisseurs de cloud public et constitue une approche plus générale des modes de gestion, de consommation et de paiement des services cloud d'une manière qui semble la mieux adaptée à une organisation donnée.

Cependant, le multi-cloud ne s'oppose pas au cloud hybride et un cloud hybride peut faire partie d'un déploiement multi-cloud. Les deux modèles ne s'excluent pas mutuellement. Le choix dépend simplement des objectifs que l'entreprise veut atteindre.

Il n'existe pas de fournisseur d'infrastructure multi-cloud unique. Adopter une stratégie multi-cloud implique généralement de combiner des services proposés par les principaux fournisseurs de cloud public, notamment Amazon, Microsoft, Google, IBM ou encore Alibaba.



KEY FIGURES

EMEA cloud adoption

The rate of cloud adoption in EMEA (Europe Middle East & Africa) slightly outpaced US and global adoption, topping 84% this year.

2016

Worldwide

59%

EMEA

66%

2018

Worldwide

81%

EMEA

84%

Source: Raiders of EMEA
Cloud Adoption, bitglass

Cloud adoption

SaaS remains the most deployed cloud model (52 percent) as software stacks are maturing, followed by IaaS (36 percent) and PaaS (28 percent), both showing strong

adoption by organizations. To a lesser extent, newer deployment models such as BPaaS (11 percent) and FaaS (10 percent) have lower rates of production deployments.

SaaS

(Software as a Service, e.g., CRM, ERP, HR apps, collaboration, productivity tools)



IaaS

(Infrastructure as a Service, e.g., servers, networking)



PaaS

(Platform as a Service, e.g., database, middleware, application servers)



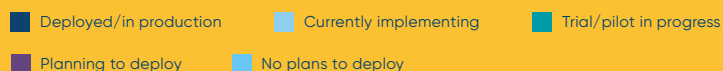
BPaaS

(Business Process as a Service)



FaaS

(Function as a Service, e.g., develop, run, and manage application functionalities)



Source: Cloud Security Report 2018: Cybersecurity Insiders

Top cloud providers

Over the past few years, public cloud providers have continued to mature and expand their service offerings. The two biggest cloud providers continue to compete for the lead in our survey:

Amazon Web Services (72 percent) and Microsoft Azure (71 percent). Interestingly, Rackspace Cloud (67 percent) displaced Google Cloud Platform (67 percent) among our survey participants to claim third place this year.



■ Current use ■ Future use

Source: Cloud Security Report 2018 :
Cybersecurity Insiders

Data in the cloud

It's no surprise that for a third year in a row, email is the most common information stored in the cloud (57 percent), a 13 point increase over last year's survey. Notably, a reversal

in trend this year, an increasing number of organizations indicate they are storing more of their intellectual property information in the cloud.

Email



Sales & marketing data



DevOps/development data



Customer data



Employee data



Contracts, invoices, orders



Financial corporate data



Intellectual property

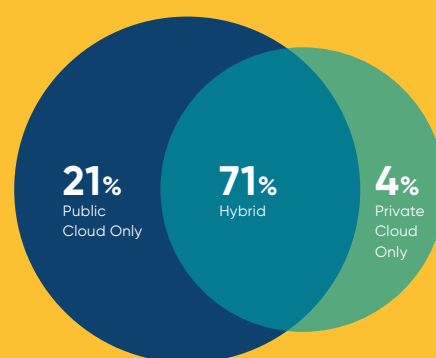


Health information



Source: Cloud Security Report 2018 : Cybersecurity Insiders

96% of Respondents Are Using Cloud



Public = 92%

Private = 75%

Both public and private cloud adoption have increased in the last year. The number of respondents now adopting public cloud is 92 percent, up from 89 percent in 2017, while the number of respondents now

adopting private cloud is 75 percent, up from 72 percent in 2017.

As a result, the overall portion of respondents using at least one public or private cloud is now 96 percent.

Source: RightScale 2018 State of the Cloud Report

Public cloud adoption

In 2018, AWS continues to lead in public cloud adoption, but other public clouds are growing more quickly.

Azure especially is now nipping at the heels of AWS, especially in larger companies.

% of Respondents Running Applications

AWS



Azure



Google Cloud



IBM Cloud



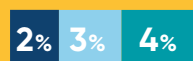
Oracle Cloud



VMware Cloud on AWS



Alibaba Cloud



Running apps Experimenting Plan to use

Source: RightScale 2018 State of the Cloud Report

% of Respondents Running Applications

AWS



Azure



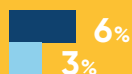
Google Cloud



IBM Cloud



Oracle Cloud



VMware Cloud on AWS



Alibaba Cloud



2018

2017

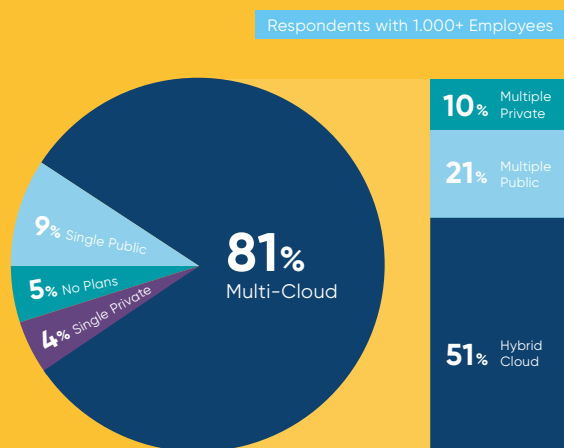
And 64 percent of respondents currently run applications in AWS, up from 57 percent in 2017 (12 percent growth rate).

Source: RightScale 2018 State of the Cloud Report

Multi-cloud is the preferred strategy among enterprises

81 percent of enterprises have a multi-cloud strategy

Enterprises with a hybrid strategy (combining public and private clouds) fell from 58 percent in 2017 to 51 percent in 2018, while organizations with a strategy of multiple public clouds or multiple private clouds grew slightly.

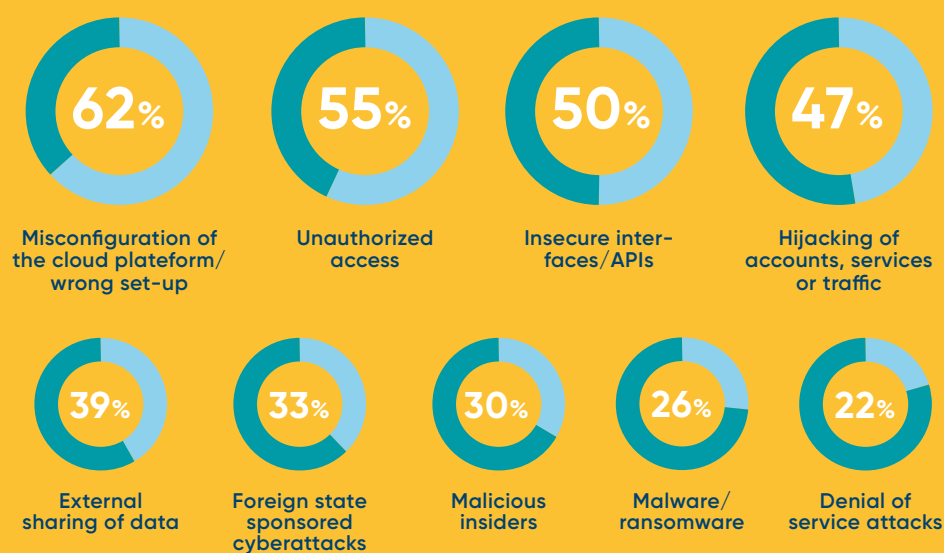


Source: RightScale 2018 State of the Cloud Report

Biggest cloud security threats

Misconfiguration of the cloud platform jumped to the number one spot in this year's survey as the single biggest threat to cloud security (62 percent).

This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).



Source: Cloud Security Report 2018 : Cybersecurity Insiders

12% Theft of service | 7% Lost mobile devices | 7% Not sure/other

CLOUD & REGU- LATION

**A POSSIBLE
MATCH!**

Comment le cloud public peut-il apporter de la valeur à l'industrie financière ? Telle est la question soulevée lors du Cloud & Regulation Event organisé par Telindus dans les locaux de la LHoFT le jeudi 8 novembre 2018. La réponse est sans ambiguïté : informatique sans serveur, extension des ressources à la demande, Intelligence Artificielle prête à l'emploi et Apprentissage Machine sont autant de vecteurs de croissance offerts par le cloud au secteur financier.

P 40

Telindus, Google & Cisco : a new era of hybrid cloud

*Bob Krentler, Head of Global Technology Alliances at **Google Cloud**, and Jeremy Oakey, Senior Director, Enterprise Product Management, Cloud Platforms & Solutions Group at **Cisco***

P 46

Cloud & Régulation: un levier pour le secteur financier

*Jacques Ruckert, Directeur Solutions et Innovation de **Telindus***

P 50

Telindus All-Clouds Offering

*Thomas Scherer, Chief Architect and **Cédric Marianacci**, Head of Department Outsourcing & Cloud Services Provider – Design and Plan at **Telindus***

TELINDUS, CISCO & GOOGLE

**A NEW ERA
OF HYBRID
CLOUD**

Like any industry, financial institutions face challenges like managing risk, striving for new sources of growth and profitability, and providing richer user experiences. But they also struggle with evolving market forces and ever-increasing regulations. On top of that, many have accumulated decades of data and must contend with hard-to-replace legacy systems. As a result, a growing number are looking to the Cloud to transform into more nimble, responsive, and creative organizations and the conversations have shifted from if they are going to, to how to move to the cloud.

Bob Krentler, Head of Global Technology Alliances at Google Cloud, and Jeremy Oakey, Senior Director, Enterprise Product Management, Cloud Platforms & Solutions Group at Cisco, took part as experts in the Cloud & Regulation event organized by Telindus on November 8th. We seized this opportunity for a thorough discussion on all the above issues, with a particular focus on the new open hybrid cloud platform stemming from a partnership between the two companies, the Cisco Hybrid Cloud Platform for Google Cloud.



Google Cloud



Jeremy Oakey, Senior Director, Enterprise Product Management, Cloud Platforms & Solutions Group at Cisco



Bob Krentler, Head of Global Technology Alliances at Google Cloud

HOW CAN FINANCIAL SERVICES PROVIDERS LEVERAGE CLOUD TECHNOLOGIES - AND PARTICULARLY MULTI-CLOUD AND HYBRID SOLUTIONS - TO DRIVE GROWTH AND DIFFERENTIATION, UNLOCK CREATIVITY, AND TRANSFORM INTO MORE AGILE, INNOVATIVE COMPANIES?

B.K. Firms across financial services are changing their approach to technology platforms. They are beginning to create, notably with Google Cloud, open hybrid architectures that can scale as needed and provide modern application development frameworks. Financial companies are also using Google's API management platform to manage ecosystems of partners that enable new product offerings and customer experiences. In this last area, tailoring to the needs of individual customers include customizing offers based on customer history and needs, enabling digital self-care through chatbots, and optimizing call center interactions to ensure fast resolution and cost effective customer service.

With Google's cloud capabilities, financial companies can identify trends through market and other external data to optimize their investment portfolios. Google's analytics solutions provide the tools and capabilities they need to ingest, transform, and analyze data - both streaming in real-time and in more traditional batch processes as well.

“ We have spent 30 billion dollars improving our infrastructure over three years. ”

Google's customers can add intelligence to risk management and compliance processes that have material impacts on their ability to proactively identify issues, from anti-money laundering to credit card and claims fraud. Google's machine learning APIs and tools provide the capability to quickly create effective risk management machine learning models.

J.O. Financial services companies are usually slower to adopt new technologies, but they also experiment very quickly. Many financial institutions have an innovation department in charge of trying the latest technologies and evaluating how they can be used. It may take some time for that innovation to make it into their applications or their production but, obviously, financial services companies are generally leaders in actually testing and trying technologies. Even for our traditional non-cloud products, like our routers, switches or servers, the financial services industry actually drives some of our newest features.

GIVEN THE AMOUNT OF SENSITIVE INFORMATION THEY HANDLE AND THEIR SPECIFIC RESPONSIBILITIES IN THIS REGARD, FINANCIAL INSTITUTIONS CONSIDER AS AN ABSOLUTE PRIORITY TO HAVE COMPLETE CONTROL OVER THEIR DATA. HOW DO YOU REASSURE THEM OVER SECURITY, PRIVACY, AND COMPLIANCE ISSUES?

B.K. Google Cloud infrastructure is custom-designed for improved performance and security. We design and include hardware specifically for security, like Titan, our custom security chip that we use to establish a hardware root of trust in our servers and peripherals. This all rolls up to our custom datacenter designs, which include multiple layers of physical and logical protection.

We champion initiatives that prioritize and improve the security and privacy of user data. Google employs expert security and privacy professionals that are tasked with maintaining the company's defense systems, developing security review processes, building stronger security infrastructure, and precisely implementing Google's security policies. We've made multiple updates to ensure that Google Cloud customers can confidently use our services now that the GDPR is effective.

Last year, we released the Google Cloud Key Management Service. With KMS, customers can manage the encryption keys used to protect sensitive data residing across the Google Cloud Platform with customer managed encryption keys.

At Google, we believe in an open cloud. We believe that openness in the cloud matters more than ever. Openness not only enables faster innovation, but it also provides tighter security and offers freedom from vendor lock-in or barriers to exit.

We have spent 30 billion dollars improving our infrastructure over three years. From datacenters to subsea cables, we are committed to connecting and serving our cloud customers. We opened our Netherlands and Montreal regions in the first quarter of 2018, followed by Los Angeles, Finland, and Hong Kong. In 2019 we will commission three subsea cables.

By deploying our own private subsea cable, we help improve global connectivity while providing value to our customers. Owning the cable ourselves has some distinct benefits. Since we control the design and construction process, we can fully define the cable's technical specifications, streamline deployment and deliver service to users and customers faster. Also, once the cable is deployed, we can make routing decisions that optimize latency and availability.

These investments further improve our network – the world's largest with over 100 points of presence and over 7,500 edge caching nodes – which by some accounts delivers 25% of worldwide internet traffic.

JO. In the security space, when it comes to having control over data, the situations are different depending on the type of service that is provided. In the case of SaaS, when using services like Salesforce.com, Office 365, or

consumer file sharing services for example, customers may not have access to all their data. With large providers like Google, the customers are actually in possession of all their data. Major public cloud players, including Google, invest more in securing their infrastructures, datacenters, and networks than most individual companies can afford.

“ At Google, we believe in an open cloud. We believe that openness in the cloud matters more than ever. ”

The first thing we must do is to get the customers comfortable with the legal frameworks in which they operate. I think this is really where a partner like Telindus comes in because they have expertise in matching what the customers are traditionally comfortable with – their contracts, their processes, their operational understanding – and what is new to them. A partner like Telindus can help customers get a better understanding of how they can use the technology, how they can effectively use the Cloud, modernize their infrastructure and their applications.



The providers actually expose quite a bit of visibility. For example, as Google owns the entire network, the traffic brought in by the customer doesn't leave the Google network to a third party until it does so by choice, by the customer's choice. Google exposes a lot of visibility into traffic flows.

Google and Cisco are working together to help customers change their security processes and retool. At Cisco for instance, we have launched Stealthwatch Cloud, which is part of our partnership and uses a new technology from Google called Virtual Private Cloud Flow Logs. VPC Flow Logs provides real-time visibility into network performance and enables network usage analysis, traffic expenses optimization, real-time security analysis, and network forensics. In this way, the customer can see exactly how services – including public cloud services – are reacting. Lots of organizations may not realize that such a level of visibility and transparency is there, it may often times require new tools to be able to extract the transparency provided by Google Cloud.

IN OCTOBER LAST YEAR, CISCO AND GOOGLE ANNOUNCED A PARTNERSHIP ON A NEW OPEN HYBRID CLOUD PLATFORM THAT WOULD BRIDGE ON-PREMISE AND CLOUD ENVIRONMENTS. THE RELEASE OF THE CISCO HYBRID CLOUD PLATFORM FOR GOOGLE CLOUD APPEARS TO BE THE FIRST STEP IN REALIZING THE POTENTIAL OF THIS COLLABORATION. WHAT ARE THE KEY CAPABILITIES OF THE JOINT CISCO-GOOGLE CLOUD SOLUTION AND WHAT ARE THE ROLE AND CONTRIBUTION OF EACH OF THE PARTNERS IN ITS CONCEPTION?

B.K. Whether they are cloud-ready or modernizing their infrastructure on-premises, many organizations can benefit from a well-supported path that lets them move to the cloud on their own terms. To address this need, we announced our partnership with Cisco last year on a new open hybrid cloud platform. The Cisco Hybrid Cloud Platform for Google Cloud is now generally available, giving our customers more options when considering hybrid solutions.



Our joint hybrid solution, the Cisco Hybrid Cloud Platform for Google Cloud, combines Cisco, Google and open source technologies to consistently and securely extend on-premise environments to Google Cloud, enabling customers to build hybrid applications.

With the Cisco Hybrid Cloud Platform for Google Cloud, applications can span across public cloud and on-premise environments to deliver speed and scale when and where needed. Applications in the Public Cloud can take advantage of on-premise capabilities including existing IT systems, and in-house applications can benefit from new cloud-native capabilities without the need for a total move to the public cloud.

This fully-integrated solution lets developers leverage enterprise-grade capabilities from Google Cloud, like managed Kubernetes, GCP Service Catalog, Cisco networking and security, and Istio authentication and service mesh monitoring.

The Cisco Hybrid Cloud Platform for Google Cloud enables businesses to accelerate on-prem application modernization using a Kubernetes-based container strategy that is consistent with cloud-native technology, including Google Kubernetes Engine. Cisco will provide a turnkey solution that is cloud-ready for Kubernetes and containers, as well as management tools to enforce security and consumption policies.

Istio's open-source technology, optimized for container and microservice, offers developers a uniform way to connect, secure, manage and monitor microservices across clouds through service-to-service level mutual TLS access control. As a result, they can easily implement new, portable services and configure and manage those services centrally.

API management through Apigee enables legacy workloads running on-prem to connect to the cloud through APIs. With Apigee, enterprises can expose legacy, on-prem services as secure APIs, to developers who can then easily incorporate these services into their modern application.

With our joint hybrid solution, Customers can extend their existing Cisco network and security policies and configurations to the cloud, and monitor application behavior across hybrid cloud environments. Besides,

“ We also work together with Google on Istio, Google's open platform to connect, monitor, and secure microservices. ”

Cisco's Technical Assistance Center provides customers with a single source of support.

Cisco is an ideal partner for us in this area because of its long-standing enterprise focus and expertise in networking, security, analytics, and hyperconverged infrastructure. The Cisco Hybrid Cloud Platform for Google Cloud offers another way to run seamlessly on-premises and in the cloud, delivering speed and scale where customers need it most. Applications in the cloud can take advantage of on-premises capabilities including existing IT systems, and applications on-premises can take advantage of new cloud capabilities—without the need for a complete shift to the public cloud.

We truly hope that the Cisco Hybrid Cloud Platform for Google Cloud makes it possible for more organizations to move to the cloud at their own pace, all while maximizing their on-prem investments and avoiding lock-in.

J.O. I must admit that it took us some time to deliver what we announced a year ago. First, because we created a new product – the Cisco Container Platform, our on-premise Kubernetes equivalent to the Google Kubernetes Engine.

We also launched new versions of products that we already had in our portfolio, but didn't support Google Cloud. We added support for Google Cloud to our Virtual Router CSR 1000V, and to the Stealthwatch Cloud product that allows to achieve visibility and threat detection in public clouds environments and between clouds. VPC Flow Logs was new for Google and launching that product was only in the works. We, Cisco, had a product that could leverage a service that Google did not offer yet. Our product, Stealthwatch Cloud, took advantage of Google developing something new. So, while Google brought new things to market, we also brought new things to market.

We also work together with Google on Istio, Google's open platform to connect, monitor, and secure microservices. They still develop a lot for Kubernetes, but their next layer on top of it is this independent service mesh that provides the fundamentals needed to architect for portability using microservices and manage large distributed deployments that span hybrid and multi-cloud deployments. From our perspective, multi-cloud was an interesting part of our collaboration with Google. Our contribution to Istio was really to help make sure that multi-cloud was something that Istio would support. We wanted to ensure that container platform would align with our multi-cloud portfolio.

It is just the beginning: we have plans to iterate and do more. We can always deepen the amount of services that we expose on-premise. For example, Google has six services today that advertise via Open Service Broker. They will continue to create more services that are available to an on-premise application. We will continue to deepen integrations like identity and security, the next area that will keep us focused. For customers to really adopt hybrid cloud, they need to have consistent role-based access control, consistent identity capability between on-premise and Google Cloud, that might mean Microsoft Active Directory on-premise synchronizing with Google Cloud identity, for example.





Our next areas of collaboration will include Edge Computing, IOT, and deepened AI/ML capabilities. The Cisco Hybrid Cloud Platform for Google Cloud also needed to be launched because of all those new capabilities, either build on top of Kubernetes or extending the framework beyond networking, security of Kubernetes itself. There will be more iteration, not only from us, but also the open source community. Projects like Istio are also being contributed to by Lyft, IBM and other technology companies working to solve the hard problems of these new cloud-native applications.

WHAT ARE THE ADVANTAGES OF CONTAINER TECHNOLOGY COMPARED WITH MORE CONVENTIONAL VIRTUAL MACHINES? AND WHAT ARE THE DRAWBACKS – SOME SAY, FOR INSTANCE, THAT CONTAINERS ARE LESS SECURE THAN VIRTUAL MACHINES?

B.K. For those coming from virtualized environments, containers are often compared with virtual machines. Like virtual machines, containers allow you to package your application together with libraries and other dependencies, providing isolated environments for running your software services. However, containers offer a far more lightweight unit for developers and IT operations teams to work with, carrying a myriad of benefits including portability across environments and agility in application development.

Google's infrastructure runs on containers and we created Kubernetes, the industry standard for orchestrating containers. The Cisco Hybrid Cloud Platform for Google Cloud is built on top of Google Kubernetes Engine and Cisco Container Platform.

Containers silo applications from each other unless you explicitly connect them. That means you don't have to worry about conflicting dependencies or resource contention: you set explicit resource limits for each service. It's an additional layer of security since your applications are not running directly on the host operating system.

The most common misconception about container security is that containers should act as security boundaries just like VMs, and as they are not able to provide such guarantee, they are a less secure

deployment option. However, containers should be viewed as a convenient packaging and delivering mechanism for applications, rather than as mini virtual machines.

In the same way that traditional applications are not perfectly isolated from one another within a VM, an attacker or rogue program could break out of a running container and gain control of other containers running on the same VM. However, with a properly secured cluster, a container breakout would require an unpatched vulnerability in the kernel, in the common container infrastructure, such as docker, or in other services exposed to the workload from the VM. To help reduce the risk of these attacks, Google Container Engine provides fully managed nodes and actively monitors for vulnerabilities and outdated packages in the VM – including third party add-ons – and performs auto update and auto repair when necessary. This helps minimize the attack window for a container breakout when a new vulnerability is discovered.

One of the downsides of running traditional applications on VMs is that it's nearly impossible to understand exactly what software is running in your production environment, let alone control exactly which software is being deployed. And because it's hard to determine the accurate states of traditional applications at scale, the typical security controls will approximate by focusing on anomaly detection in application and OS behaviours and settings.

In contrast, containers provide a more transparent, easy-to-inspect and immutable format for packaging applications, making it easy to establish a workflow to inspect and catalogue container content prior to deployment.

J.O. A container is a running application that has mobility to it. What I mean by mobility is that a container works equally on-premise – on the Cisco Container Platform – and on Google Cloud. Virtual Machines usually had a very specific technology – VMware used a different format than Amazon, than Google, than Azure. Containers have more portability because there is a consistent framework.



There are some nuances in that. Containers are not automatically movable. We do act like they are, but there are still some challenges with them, such as making it easier to connect services. There is work in the actual container runtime to make it more consistent between public cloud and on-premise.

The drawbacks for containers can be anything. You can take a Virtual Machine and put it in a container, but that's not a microservice; it's a very, very large container! This is the first reaction of some customers when they start experimenting with containers. I don't think that's right or wrong, but that's not a microservice, that's not part of a cloud-native application.

Virtual Machines were really part of a previous application architecture where the application received its resiliency and recovery capabilities from the infrastructure. There was a much hardwired design relationship between the application and the infrastructure. Containers, in and of themselves, don't solve that problem. But cloud native applications, microservices and this new design pattern

of applications being resilient within themselves and having cloud scale capabilities, is really what is unique about containers. A customer who is not learning what it means to have a cloud-native application and not refactoring his applications to microservices is not truly understanding the power of containers.

With Kubernetes, I can do rolling upgrades of the infrastructure and the application is unaware of that. It's different in Virtual Machine. VMs often times needed very advanced capabilities to have that resiliency because the application would brake if one server went down. In the Kubernetes world, one server or one container can go down and the architecture doesn't fix the problem. The application design actually makes the application resilient.

TELINDUS TOOK PART IN GOOGLE'S EARLY ACCESS PROGRAM. WHAT ROLE DID THEY PLAY AND WHAT DID THEY BRING MORE SPECIFICALLY? WHAT ARE THE NEXT PLANS WITH REGARD TO THE CISCO, GOOGLE AND TELINDUS PARTNERSHIP?

B.K. Telindus is an integrator and cloud service provider working in security-sensitive and regulated industries with a well-established reputation for being an early adopter of new technologies. The role played by Telindus as a participant in the Early Access Program enabled the deployment of a Cisco Hybrid Cloud Platform for Google Cloud environment, leveraging on-premise infrastructure to access Google Cloud. The new technologies that the Early Access Program used included Cisco Container Platform, Open Service Broker, and Istio.

The Telindus deployment is a great example of how service providers can use a hybrid cloud environment to help customers transparently extend their datacenters to harness rich, cloud-based services and tools, enabling them to develop and deploy applications on premises, while leveraging best-of-breed public cloud tools at the same time.

“ An attacker or rogue program could break out of a running container and gain control of other containers running on the same VM. ”

Telindus has been offering container-based platforms for several years and we have worked with them to define a solution that addresses a need in the market for on-premises, service provider-based deployments. The Hybrid Cloud Platform is the right vehicle for Telindus because it lets them enable modern container-based solutions in environments where security and robustness is an integral part of technical deployments. This is because of the Hybrid Cloud Platform's private-hosting capabilities

for security-sensitive workloads. Also, the out-of-the-box portability to and from the public cloud enables disaster recovery, vendor-lock-in mitigation, and scalability. This is especially important for Telindus' regulated customers, who might not be able to work directly with public cloud providers, to transition to cloud.

The Hybrid Cloud Platform's use of open source technologies like Istio, Kubernetes, and Open Service Broker which can be used in any hosting environment, are key. The integration of Cisco CloudCenter provides policy-based automation governance of multi-tier microservice architectures from within the private infrastructure that are deployable into the public cloud. The Hybrid Cloud Platform solution made it possible for Telindus to build a cloud-native, on-premises experience, which can be easily scaled out into the public cloud, with XaaSification features for legacy and container-based services.

The Cisco Hybrid Cloud Platform for Google Cloud has been tested and field trialed with the help of partners like Telindus. The platform is now certified to be consistent with Google Kubernetes Engine, enabling GCP out of the box, and it's fully ready for customers' production workloads.

Today, Telindus is able to use this deployment to help customers seamlessly extend their datacenters and accelerate their application innovation. We are really excited about Telindus' ability to bring an open hybrid cloud to financial services customers through their digital transformation journeys.

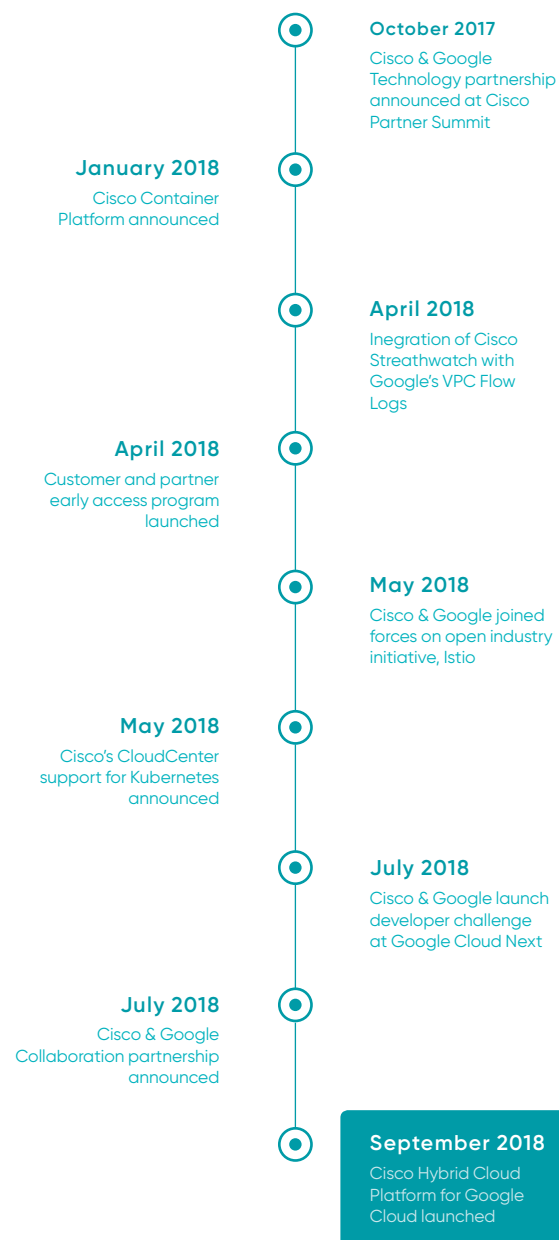
J.O. Telindus has been a strong Cisco partner for many years, before containers, virtual machines and even the Internet were born. With partners like Telindus, we help each other innovate to take on the new challenges and transform ourselves as the industry changes. A partner like Telindus brings us scale because we don't have the reach to touch every single customer. We have Cisco products in over 80% of the Internet – connected customers are using Cisco routers, switches, or firewalls. We, Cisco alone, cannot touch all those customers, understand their business, react to their requirements, deliver the services they need and educate them on what we are doing. A partner like Telindus helps us bring scale to everything we do.

As we start a new venture, like we did with Google, and launch new software products, having a partner like Telindus participate in an Early Access Program helps us because they bring a vertical perspective to industry. As experts, they can give us feedback on our assumptions and validate our use cases. In return, participating in the program is valuable for Telindus as well because they can touch and learn the technology before everyone else. And when we actually launch it on the market, they have already been able to imagine how they could build services around that product and integrate it with other products. Having access to the product early helps them in their business as well.

Cisco Container Platform is releasing every month. We are only up to 2.0 and 2.1 will be out in a couple of weeks. Telindus has seen nine or ten releases of the product whereas most others have only seen one or two. Telindus has helped shape how the product is going. They are also still seeing the new releases quickly and they already have the knowledge of the past to help them pick up the new features immediately.

We are also starting to see enterprise software companies rewriting their applications to be containerized. Telindus is positioned to pick up these new enterprise applications, integrate them in their own portfolio and develop their own solutions. For example, we have recently completed the acquisition of Duo Security, which allows us to add unified access security and multi-factor authentication to our stack and to multi-cloud. You can expect to see other multi-cloud-focused software acquisitions and Telindus will be well positioned to help us scale and deliver those products to the customers.

Cisco & Google Partnership Milestones



CLOUD & REGLE- MENTA- TION

**UN LEVIER
POUR LE
SECTEUR
FINANCIER**

La réglementation est souvent perçue comme un obstacle à l'adoption du cloud. Telindus y voit au contraire un moyen de fournir des solutions cloud de manière efficace et sécurisée. Pour Jacques Ruckert, Directeur Solutions et Innovation de Telindus, quand le cloud s'accorde avec la réglementation, en particulier dans le cadre de l'industrie de la finance, la somme des deux constitue un catalyseur d'innovation et un levier de développement pour les entreprises.

COMMENT LE CLOUD PUBLIC PEUT-IL AIDER LES ENTREPRISES DU SECTEUR FINANCIER À RÉDUIRE LEURS COÛTS OU À GÉNÉRER DE NOUVEAUX REVENUS ? QUELS AVANTAGES SUBSTANTIELS APPORTE-T-IL ?

J.R. Le cloud public permet d'automatiser entièrement l'exécution de nombreuses opérations et d'alléger les charges d'exploitation au quotidien. Les entreprises peuvent ainsi concentrer leurs ressources sur les outils informatiques qui animent le cœur de leur métier. Une stricte séparation entre données et calcul permet de créer des services afin de ne traiter les données que lorsque c'est réellement nécessaire. Les entreprises ont également la possibilité de créer un "pipeline" de traitement de données, un cluster Hadoop par exemple, de l'utiliser pendant qu'elles travaillent réellement sur ces données et de le supprimer par la suite, et cela sans coût permanent et sans infrastructure à gérer.

D'autre part, les énormes réserves de capacité que possèdent les grands acteurs du cloud permettent de bénéficier de modèles de facturation à l'usage qui s'avèrent financièrement très intéressants. Les entreprises peuvent par exemple faire travailler des centaines de serveurs pendant une heure plutôt qu'un seul serveur pendant des centaines d'heures pour le même prix et réaliser ainsi d'énormes gains d'efficacité. Les dernières innovations visant à paralléliser les tâches – et il ne s'agit plus ici de théorie – permettent de traiter de grandes quantités de données en temps réel. On peut de la sorte obtenir de précieuses informations commerciales en analysant des données financières en quasi-temps réel, ce qui aurait pris des jours, voire des semaines, il y a quelques années.

Cet accroissement de l'extensibilité des ressources a autorisé le déploiement de technologies capables d'analyser les données dans des délais très courts. Google a mis cela en pratique dans son cloud en créant notamment des modèles d'apprentissage machine destinés aux organisations qui ne disposent pas de spécialistes en science des données.

Il existe en outre de nombreux modèles prêts à l'emploi, comme ceux qui sont utilisés aujourd'hui quotidiennement pour la reconnaissance vocale et textuelle, la traduction ou la reconnaissance faciale. Ces API (Applications Program Interface) sont faciles à intégrer dans les applications métier, autorisant les entreprises à créer leur propre solution d'intelligence artificielle sur mesure pour leur cœur d'activité.



Jacques Ruckert, Directeur Solutions et Innovation de Telindus

MAIS QU'EN EST-IL ALORS DE LA CONFORMITÉ RÉGLEMENTAIRE ET DE VALEURS COMME LA CONFIANCE ET LA FIABILITÉ SUR LESQUELLES SE FONDE LA RELATION PRIVILÉGIÉE QUE LES BANQUES ENTRETIENNENT AVEC LEURS CLIENTS ?

J.R. Les banques opèrent effectivement dans un environnement fortement réglementé. Leur principale responsabilité est de gérer les actifs de leurs clients. En conséquence, les institutions financières sont également responsables des infrastructures informatiques qui constituent le pilier sur lequel reposent leurs activités. Elles doivent donc veiller à apporter des réponses à une série de questions-clés relatives, entre autre, à la localisation des données et à leur contrôle, au respect de la confidentialité des données privées, à la traçabilité des opérations, à la chaîne de sous-traitance, à la résilience des systèmes, ou encore à la prise en compte d'une stratégie de sortie vis-à-vis d'un fournisseur. Cette liste est loin d'être exhaustive.

“ Telindus se positionne comme un accélérateur de la transformation cloud pour les institutions financières ”

Il y a plus de 15 ans, le Luxembourg s'est doté d'un cadre juridique autorisant l'externalisation de systèmes informatiques par les institutions bancaires. Cette législation spécifique est applicable aux prestataires de services qui concluent des accords d'externalisation avec l'industrie financière. Ces prestataires sont réglementés afin de réduire les risques opérationnels et les violations de confidentialité. Le mot-clé de ce cadre réglementaire qui a favorisé l'éclosion d'un véritable écosystème autour du secteur financier est "PSF", Professionnel du Secteur Financier. Concrètement, cela signifie qu'un fournisseur de services – de services informatiques dans le cas qui nous concerne – est obligé d'obtenir un agrément de la part du régulateur financier pour être autorisé à fournir ses services à une banque.

Le dernier aménagement apporté à ce dispositif réglementaire est la circulaire CSSF 17/654, dite "Circulaire Cloud", qui s'applique à toute institution financière souhaitant externaliser des services informatiques vers une infrastructure de cloud. Cette circulaire permet à une entité réglementée, c'est-à-dire une institution financière ou un PFS, de recourir à des services de cloud public moyennant l'observation de règles de gouvernance strictes.

En résumé, il existe donc aujourd'hui au Luxembourg une législation cohérente à laquelle doivent se conformer les institutions financières et les PSF qui souhaitent externaliser des services informatiques vers le cloud public. Cette réglementation garantit le respect d'un certain nombre d'obligations et de valeurs. Chez Telindus, nous avons mis en place un cadre opérationnel et contractuel pour répondre à ces éléments-clés. De plus, nous sommes convaincus que ces valeurs sont tout aussi pertinentes pour d'autres secteurs d'activité, eux aussi hautement sensibles sur le plan de la sécurité et de la confidentialité. Nous le constatons à travers le dialogue permanent que nous entretenons avec nos clients non réglementés.

QUEL EST L'ÉTAT DE LA QUESTION AU NIVEAU DE L'UNION EUROPÉENNE ?

J.R. L'Autorité Bancaire Européenne, dont la mission est de renforcer le système européen de supervision financière, a récemment publié un ensemble de recommandations à l'intention des banques qui désirent externaliser leurs services auprès de fournisseurs de services cloud. Nous avons constaté avec satisfaction que la correspondance était quasiment parfaite entre les recommandations de l'ABE et les directives de la CSSF. Cela confirme que le Luxembourg se situe à l'avant-garde de l'externalisation réglementée vers le cloud dans le secteur financier. C'est un atout pour Telindus car, même si toute banque européenne est bel et bien sous la supervision de son régulateur national, nous pouvons faciliter le passage au cloud d'une institution financière en Europe, puisque nous sommes de facto conformes aux recommandations de l'ABE.



QUELLE EST LA PERCEPTION DE TELINDUS DE CE MARCHÉ RÉGLEMENTÉ ? QUEL RÔLE ENTENDEZ-VOUS Y JOUER ET DE QUELS MOYENS DISPOSEZ-VOUS ?

Nous voyons la réglementation comme un levier et le rôle de Telindus comme celui d'un catalyseur, d'un accélérateur de la transformation cloud pour les institutions financières. Telindus se positionne comme un intermédiaire entre la banque et le fournisseur de services de cloud public.

Nous combinons les atouts du cloud public avec les capacités de nos propres infrastructures d'hébergement pour permettre le traitement de données provenant d'infrastructures privées par exemple, ou pour aider à mettre en place des stratégies de sortie réellement efficaces. Nous y travaillons notamment avec notre partenaire Cisco en nous appuyant sur ses solutions réseau et serveur. Les nouveaux produits de Cisco centrés sur le cloud permettent en effet d'établir une cohérence entre les clouds publics et privés et de piloter l'ensemble à travers un tableau de bord unique.

“ Nous voyons la réglementation comme un levier ”

Nous avons en outre mis en place le cadre contractuel nécessaire avec notre partenaire et fournisseur de services cloud Google. Nous pensons que le cloud Google constitue un cloud adéquat pour le secteur financier, non seulement en raison de la position privilégiée de celui-ci en matière de traitement de données, mais aussi et surtout de par son approche fondée sur l'open source, ce qui facilite l'implémentation d'une stratégie de sortie. Nous sommes convaincus que la liberté de choix des clients et la flexibilité sont ce qui importe le plus pour Google, sans oublier les niveaux de sécurité élevés qu'offrent ses infrastructures. Google est par exemple le seul grand fournisseur de services cloud à disposer de son propre réseau backbone pour interconnecter toutes les régions où il opère.

TELINDUS ALL-CLOUDS OFFERING

By leveraging U-flex, its own Luxembourg-based private cloud, and partnerships with leading public cloud providers, Telindus offers its customers hybrid and multicloud solutions that enable them to achieve sustainable cost reductions and exploit new business opportunities. Thomas Scherer, Chief Architect, and Cédric Marianacci, Head of Department Outsourcing & Cloud Services Provider – Design and Plan, shed light for us on the all-clouds strategy devised and pursued by the company.



Thomas Scherer, Chief Architect at Telindus

WHAT ARE THE SCALE AND SCOPE OF TELINDUS' HYBRID CLOUD OFFERING?

T.S. Under Telindus' hybrid cloud we offer our consulting, integration and operation services using a single or a combination of cloud hosting infrastructures. In terms of private cloud, we are able to build dedicated private cloud hosting infrastructures at our customer's premises or in our datacenters, or leverage on our U-flex infrastructure, which is our private managed cloud platform offering.

In terms of public cloud, we have developed partnerships with three of the leading global providers. This opens the door to massive amounts of IaaS, PaaS and SaaS products, which we can bring to our customers. All these products have their specific strength. Therefore, we seek to work together with our customers already at an early stage of their cloud journey, to identify the best options for them.

Complexity is significantly reduced, notably when using public cloud services. However maintaining a consistent IT and security architecture across multiple clouds is not necessarily a given. Therefore, we have built up solutions to allow unified cloud services management independently of the private or public clouds in use. This includes, among others, cloud-agnostic service deployment and lifecycle management, data replication and backup, monitoring, security configuration as well as running VPN or private connectivities across those hosting infrastructures.

WHAT PARTNERSHIPS DID YOU FORM IN TERMS OF PUBLIC CLOUD?

T.S. We partner with Microsoft Azure, Google Cloud Platform and Amazon Web Services because we do not believe that there is a one-fits-all cloud. On top of that, we are convinced that flexibility in vendor selection is crucial for our customers. There is certainly a portfolio overlap between these providers, notably when it comes to IaaS components, yet they all have their individual strengths. For example, AWS has a remarkable range of services while Google has impressive solutions for TPU-based¹ machine learning in combination with their own inter-regional backbone. Microsoft Azure and O365 are well adopted for enterprise usage and are notably strong out-of-the-box for hybrid usage through Azure Stack, which we offer as a service from Luxembourg.



Cédric Marianacci, Head of Department Outsourcing & Cloud Services
Provider - Design and Plan

WHAT DOES TELINDUS' PRIVATE MANAGED CLOUD SERVICES PORTFOLIO CONSIST OF?

C.M. Our private managed cloud platform, U-Flex, is fully redundantly hosted across two Tier IV datacenters in Luxembourg. U-Flex offers flexible combinations of housing, dedicated and shared infrastructure hosting solutions as well as numerous managed services, such as managed databases, managed security services -

firewalling or proxy services - but also common enterprise solutions like email, collaboration or telephony services.

But this flexibility does not end with the infrastructure hosting options: our teams are able to support our customers in the daily management of their IT landscape, whether it is based on dedicated or shared workloads. This day-to-day management is designed in such a way that the services can be expanded into the public cloud, creating the foundation of our hybrid cloud offering by providing overall IT and security consistency and thereby portability of services.

WHAT ARE THE ASSOCIATED CONNECTIVITY CAPABILITIES?

C.M. Reliable connectivity is often key for hybrid deployments. Hence, we offer private WAN solutions to interconnect on-premise deployments with U-Flex and all public clouds in a fully meshed mode. This also includes the possibility to establish private WAN connectivity for the public cloud providers' inter-regional traffic.

TELINDUS OFTEN PRESENTS ITSELF AS A CLOUD TRANSFORMATION FAST TRACK FOR FINANCIAL SERVICES INSTITUTIONS. HOW DO YOU FACILITATE THE TRANSITION TO THE CLOUD FOR THOSE FIRMS?

T.S. Telindus is supervised by Luxembourg's financial regulator for providing IT services to financial institutions. In 2017, the regulator has published a circular governing the use of public clouds by financial institutions. When using public clouds, a number of conditions have to be fulfilled in order to ensure control over data and IT infrastructures. We have put in place the necessary controls to meet those control requirements. This can be on a contractual basis - such as audit rights for instance - or on a technical basis - mitigating lock-in risk or controlling data location for example. We have proactively created the necessary contractual and technical framework so that our customers do not need to handle the fulfilment process by themselves anymore. It turns out that this set of measures is not only an asset for financial institutions, but also for our customers in general as it enables secure and controlled usage of clouds.

¹ The Tensor Processing Unit (TPU) is a custom ASIC chip designed by Google for machine learning workloads.
Source: «What makes TPUs fine-tuned for deep learning», Google Cloud

CASE STUDY *KNEIP*

**KNEIP ENTRUSTS
THE PROTECTION
OF THEIR DATA
TO TELINDUS**



KNEIP's goals

- Bring in a provider capable of supporting the digital transformation currently taking place, particularly in the area of security
- Have a trusted third party through which secured services may be delivered
- Leverage on a company with sound experience in the field of information security services outsourcing
- Allow internal teams to focus on the delivery of services to customers
- Enable the delivery of clean and meaningful data
- Avoid inflation of in house back office staff and resources
- Deliver an added-value service at the right price point

The challenges

- KNEIP is a well known name in Luxembourg's financial services landscape and security is an integral part of their brand
- KNEIP's customers are very sensitive to information security matters
- KNEIP must be able to prove and demonstrate to its customers that it meets auditing requirements
- Data volume issue: ensure the security of the huge amounts of data that KNEIP must process
- Find the right "signal-to-noise" ratio between relevant security alerts, considerable quantities of false-positives, and alerts on less useful or non-sensitive data
- Ensure a high level of security while keeping the internal resources and head count at the right level
- Data categories issue: take into consideration a three dimensional view composed of infrastructure, service, external (client) and internal (user) access, and determine normal behaviours for the different roles involved

The solution

- A customised and compliant security solution based on the Cyber Security & Intelligence Operations Center (CSIOC) owned and operated by Telindus in Luxembourg
- Log management is the foundation of CSIOC activities. Working closely with KNEIP's teams, Telindus security engineers have initially defined the perimeter to be covered in order to collect the information relevant for investigation
- Proactive protection is based on business behaviour and risks. Telindus security engineers have set up use cases aligned with KNEIP's risks and constantly monitor business activities to detect suspicious events
- 24/7 real-time monitoring by engineers based in Luxembourg
- Incident management: governance, processes, and strong SLAs ensure the efficiency of the response in case of incident.
- Security Watch: on a regular basis, Telindus security engineers adapt their CSIOC services according to KNEIP's activities and new indicators of compromise (IOC)
- Scalable services based on changes in KNEIP's activities while keeping the allocated budget under control



The results

- High quality output in terms of reporting and alerting
- Monthly CSIOC report review with Telindus security engineers in order to benchmark the actual situation against predefined metrics and KPIs
- Permanent support of Telindus in the continuous improvement of KNEIP's threat detection capabilities
- Fully demonstrable and auditable solution, from the alert raised by Telindus to the closing of the incident ticket, through the investigation phase
- Real time monitoring and alerting on events happening outside of the predefined framework
- Balanced "signal-to-noise" ratio resulting in actionable information for KNEIP teams
- Optimum management of the volume of data
- Continuous feedback loop across the company and with Telindus in order to improve the service from both sides

The benefits for KNEIP

- Superior service that adds value to the company
- Information provided by Telindus is prequalified, helping KNEIP significantly reduce “time-to-diagnosis” and therefore improving the fluidity of service and reducing operating expenses
- Trustworthy PSF partner with an active commitment
- Control and transparency of the cost of the solution
- Limited investments in internal resources and staff
- Continuous security watch

Discovery their story



“This security outsourcing service was the first occasion for me to collaborate with Telindus. Since then, I have worked with Telindus on several projects, all of this confirming their flexibility and willingness to build a true partnership, along with their deep sense of honesty and accountability”

*Kevin Brannigan,
Head of Engineering Operations, KNEIP*



“One of the key elements I take away from our collaboration with Telindus is their willingness to listen to our own suggestions and initiatives, which is not only a plus for us as a client but also helps our company make the service we provide to our customers more efficient”

*Marco Zeimantz,
Engineering Operations Senior Manager, KNEIP*

About KNEIP

KNEIP was incorporated in 1993 providing publication services to the fund industry. Currently KNEIP has offices in six locations (Luxembourg, the UK, Germany, France, Belgium, Switzerland), and the company's team is composed of 263 specialists who service investment funds around the

globe. KNEIP is supervised by the Luxembourg CSSF, has the status of Professionnel du Secteur Financier (PSF), and is ISAE3000/ SSAE16 Certified. KNEIP serves over 400 asset management companies having combined assets under management of €1.8 trillion.

“ Security is at the heart of everything we do ”

Kevin Brannigan, Head of Engineering Operations, KNEIP

CSIOC*

SÉCURISER LA TRANSFOR- MATION NUMÉRIQUE



Frédéric Hauss, Responsable des opérations du CSIOC

*Olivier Trientz, Responsable commercial des services de
Cybersécurité & CSIOC*

Nul ne peut contester les avantages apportés à l'économie numérique par le cloud sous toutes ses formes. Pourtant, en ouvrant comme jamais l'entreprise au monde extérieur, les technologies et les services cloud risquent d'exposer celle-ci à des problèmes de sécurité inédits ou d'une ampleur sans précédent. Le Cyber Security & Intelligence Operations Center (CSIOC) de Telindus permet de mettre en place une surveillance et des moyens d'action adaptés à cette nouvelle réalité, ainsi qu'une gouvernance et des processus autorisant une réaction rapide et efficace en cas d'alerte. La sécurité est au cœur de la stratégie de Telindus, ce qui se confirme par la récente certification ISO27001 de ses services de Cybersécurité. Olivier Trientz, Responsable commercial des services de Cybersécurité & CSIOC, et Frédéric Hauss, Responsable des opérations du CSIOC, nous en exposent la dynamique.

NOC, SOC, CSIOC,... QUELLES RÉALITÉS SE CACHENT DERRIÈRE CES ACRONYMES ?

Olivier Trientz Le NOC - Network Operations Center - exerce une forme de monitoring afin de garantir la disponibilité du réseau, des systèmes et des communications. Sa principale fonction est d'assurer un service réseau ininterrompu. C'est avec le SOC - Security Operations Center, que l'on entre dans le domaine de la détection de comportements malicieux.

Frédéric Hauss De manière plus formelle, on peut dire que si la sécurité des systèmes d'information repose sur quatre piliers - la confidentialité, l'intégrité, la disponibilité et la traçabilité - le NOC assure l'aspect disponibilité, alors que le SOC adresse ces quatre besoins à la fois. Quoi qu'il en soit, le NOC et le SOC se complètent et travaillent en tandem pour assurer les opérations et la sécurité de l'ICT.

Quant au CSIOC, il s'agit d'un SOC auquel on ajoute une dimension "Cyber", ce qui souligne qu'aujourd'hui à l'ère du cloud, notre SOC ne se limite plus seulement au périmètre de l'entreprise. La responsabilité de la sécurité de celui-ci en revient donc au fournisseur de services cloud, comme c'est le cas pour Telindus.

LEUR CHAMP D'ACTION SEMBLE LÉGÈREMENT VARIER, MAIS QUEL EST LEUR POINT COMMUN ?

F.H. Derrière les machines il y a des hommes. Les SOC et leurs déclinaisons sont avant tout une affaire de spécialistes. En effet, même si ces services s'appuient sur de nombreuses solutions de sécurité, ils sont surtout délivrés par des experts de haut niveau capables d'analyser une masse d'information pour en extraire des comportements inhabituels, et pour ceux jugés malicieux, de créer de nouveaux scénarios de détection accompagnés d'un plan de remédiation théorique qui par la suite, sera adapté à la situation réelle du client.

O.T. L'objectif premier est d'assurer la continuité des activités et la survie de l'entreprise en cas d'incident. Pour cela, la clé est de raccourcir le délai entre une attaque et sa détection, afin de se laisser un temps précieux pour déployer le plan et les capacités de réaction et de remédiation adaptés à la menace.

Cette course contre la montre nécessite une bonne préparation, mais également un pilotage précis des indicateurs de sécurité depuis un SOC global, qui devient la tour de contrôle de la sécurité de toute l'entreprise.

“ En effet, même si ces services s'appuient sur de nombreuses solutions de sécurité, ils sont surtout délivrés par des experts de haut niveau ”

QUELLES FORMES LES VIOLATIONS DE SÉCURITÉ PRENNENT-ELLES À L'HEURE ACTUELLE ?

O.T. D'après notre expérience, 80% des violations de sécurité constatées aujourd'hui trouvent leur origine à l'intérieur de l'entreprise, soit via des pièces rapportées par des visiteurs ou des intervenants externes, soit par maladresse ou négligence – lorsqu'un développeur lance une application de scanning du réseau sans autorisation préalable, par exemple – soit encore par malveillance. Ces brèches de sécurité accidentelles ou intentionnelles peuvent se traduire par des fuites de données ou l'introduction d'un malware.

F.H. Les attaques qui ont un impact important proviennent en effet de l'intérieur de l'organisation. Depuis l'extérieur, il s'agit le plus souvent d'opérations frauduleuses d'extorsion d'argent sous ses multiples formes, comme par exemple des versions revisitées de ransomware.

Ces attaques extérieures sont dorénavant très ciblées, jusqu'à ne viser parfois qu'une seule entreprise. Il peut s'agir d'attaques DDoS conduites à l'aide de botnets composés de machines zombies, ou d'attaques sans logiciel malveillant, comme dans le cas du phishing.



SUR QUELLES BASES LE CSIOC DE TELINDUS A-T-IL ÉTÉ CRÉÉ ?

F.H. Le CSIOC de Telindus trouve son origine dans la nécessité d'adapter la protection actuelle de notre cloud aux nouvelles cyber-menaces et aux vulnérabilités croissantes de par l'augmentation constante du nombre des équipements à couvrir. Ainsi pour améliorer notre proactivité et réactivité nous avons décidé de centraliser sous une coupole unique diverses compétences, expertises et sources d'informations disséminées jusque-là dans toute l'entreprise.

C'est là que le "I" de CSIOC – pour Intelligence, au sens renseignement du terme – prend tout

son sens puisqu'il désigne notre volonté de proactivité vis-à-vis des menaces, à travers une veille continue du monde de la cybercriminalité, un univers très actif et en évolution permanente. Nous adaptons sans cesse nos scénarios de détection en fonction de cette évolution et, surtout, nous les adaptons aux activités de nos clients. Ce dernier est un élément différenciateur propre à notre approche qui est primordial pour assurer la sécurité de nos clients.

O.T. Les entreprises qui s'adressent à nous ont déjà dépassé la question de savoir s'il est opportun de développer un SOC en interne. Cette option nécessite en effet de mettre en place toute une

série d'outils qui représente un investissement conséquent en matériels comme en logiciels. De plus, il faut disposer des ressources nécessaires pour opérer une telle structure, c'est-à-dire des experts et une organisation prête à réagir 24 heures sur 24. Nos clients sont donc conscients qu'ils doivent se tourner vers un acteur externe pour assurer la sécurité de leurs infrastructures et de leurs données pour concentrer leurs ressources sur leurs activités core-business.

Telindus dispose des moyens nécessaires pour faire face à ce type de demande. Ces moyens se traduisent par la mise à disposition d'une équipe d'experts et d'une infrastructure soit mutualisée, soit dédiée, selon les besoins des clients. C'est ce qui rend notre offre attrayante : nous sommes capables d'assurer la mise à disposition des infrastructures - hébergées dans nos centres de données de niveau Tier IV - comme des spécialistes indispensables pour garantir à nos clients la haute disponibilité de leurs systèmes d'information.

“ L'objectif premier est d'assurer la continuité des activités et la survie de l'entreprise en cas d'incident.”

A QUELS TYPES D'ENTREPRISES VOS SERVICES S'ADRESSENT-ILS ?

O.T. Nos services s'adressent à des organisations de toutes tailles et de tous secteurs: assurance, finance, commerce, service, ou encore industrie.

Les premiers dossiers sur lesquels nous sommes intervenus nous ont d'ailleurs été confiés par des entreprises industrielles déterminées à se prémunir contre tout arrêt de production mais aussi contre l'espionnage industriel et le vol de secrets commerciaux.

Dans le secteur de la finance, le régulateur augmente progressivement les exigences en matière de sécurité. Dans ce contexte, quelle que soit la taille des banques, toutes doivent se conformer aux mêmes contraintes réglementaires, comme par exemple les contraintes PSF, SWIFT ou GDPR. Le caractère évolutif de l'offre de Telindus permet de dimensionner au mieux la solution à mettre en place en fonction du profil de l'institution et de ses risques métier. Nous préconisons généralement d'établir d'abord une supervision périmétrique, pour s'assurer une surveillance des communications entre l'infrastructure et le monde extérieur, et de cibler ensuite certaines applications spécifiques ou critiques pour l'activité de celle-ci.

QUELLE EST VOTRE APPROCHE CONCRÈTE SUR LA MISE EN PLACE D'UNE SOLUTION DE SÉCURITÉ ?

F.H. Chacune de nos missions débute par l'identification des scénarios à risque auxquels doivent faire face les clients, ainsi que par l'analyse des communications réseaux et de l'architecture de l'infrastructure. Au final, l'objectif est d'établir une baseline des comportements réseau et business, qui permettra par la suite de déceler la présence éventuelle d'une anomalie. Au fil du temps, nous développons une connaissance approfondie de l'environnement de nos clients qui nous permet d'identifier tout comportement inhabituel : communications vers d'autres parties du monde ou communications internes de machine à machine, par exemple. Chaque événement est analysé pour différencier le normal de l'anormal. C'est d'ailleurs la marque de fabrique du CSIOC de Telindus.

O.T. L'effort de proactivité qui précède toute détection éventuelle d'une anomalie est très important chez Telindus. Cela implique de comprendre les activités de nos clients ainsi que les flux de communication, d'être en relation constante avec eux et d'accompagner l'évolution de leur infrastructure et de leur parc applicatif afin d'être dans les bonnes conditions pour réagir de manière appropriée lorsqu'une alerte survient.



**EN PLUS DES CONNAISSANCES
TECHNIQUES ATTENDUES,
DE QUELLES COMPÉTENCES
GÉNÉRALES LES MEMBRES DE
L'ÉQUIPE CSIOC DOIVENT-ILS
FAIRE PREUVE ?**

F.H. La qualité primordiale que nous recherchons chez un analyste, c'est une grande capacité de communication, indispensable pour entretenir l'interactivité entre les équipes. Nos collaborateurs doivent également être capables de gérer une situation dans le stress : chez Telindus, il faut réagir à un incident en l'espace d'une demi-heure. Tel est notre engagement vis-à-vis de nos clients.

Nous avons mis en place trois niveaux d'expertise parmi nos analystes. Le SOC regroupe les spécialistes de niveaux 1 et 2. C'est l'équipe du CSIRT (Cyber Security Incident Response Team) de Telindus qui fournit nos spécialistes de niveau 3, lorsque cela s'avère nécessaire :

- Un spécialiste de niveau 1 doit être capable d'analyser une situation très rapidement afin d'effectuer un premier tri parmi les alertes. A ce niveau, les capacités que nous recherchons sont la résistance au stress, l'exactitude dans l'analyse et le sens de la communication. Un analyste de niveau 1 doit être capable de travailler rapidement et savoir quand passer la main à un niveau supérieur.

- Le spécialiste de niveau 2 a pour rôle d'analyser en profondeur les incidents qui lui sont remontés afin d'en déterminer la cause, de communiquer cette information au client et d'aider à mitiger les effets.
- Par la suite, l'équipe de forensics de Telindus, qui relève du niveau 3, peut être appelée à rechercher la root cause de l'incident de sécurité, à savoir la "cause derrière la cause".

Une équipe d'une dizaine de personnes assure ainsi une couverture à 360°, à travers les trois niveaux d'expertise, en assurant un service 24/7.

O.T. En tant qu'intégrateur, Telindus dispose également d'une équipe d'ingénieurs réseau et sécurité bénéficiant d'une grande expérience sur le terrain et d'un large éventail de certifications techniques. Cette équipe est prête à intervenir à tout moment, de jour comme de nuit, pour aider nos clients à mettre en œuvre les mesures préconisées, qu'il s'agisse de modifier certaines configurations, de mettre en place une règle de firewall ou d'appliquer des patchs de sécurité pour contenir et réagir aux incidents chez nos clients.

F.H. En complément de notre offre, nous proposons des services à valeur ajoutée tels que des analyses périodiques comparatives de vulnérabilités, des tests d'intrusion et Red Team, des actions de Threat Hunting destinées à identifier

les attaques persistantes avancées ou les tentatives d'exfiltration de données, ou encore des campagnes de phishing, ces dernières portant plus particulièrement sur le maillon humain de la chaîne de sécurité.

A ce niveau, nous pouvons mettre en œuvre certaines tactiques de Threat Intelligence qui consistent à attirer des adversaires déclarés ou potentiels sur des ressources spécifiques sous contrôle afin d'identifier ces attaques avancées. Le but de ce leurre est de faire croire aux attaquants qu'ils peuvent prendre le contrôle d'une véritable machine de production, ce qui permet à nos experts d'observer les moyens de compromission utilisés et de prémunir l'infrastructure de nos clients contre de nouvelles attaques.

LA COMPLEXITÉ ACCRUE QUI SOUS-TEND L'APPROCHE MULTI-CLOUD EST-ELLE SUSCEPTIBLE D'ENTRAÎNER D'AVANTAGE DE PROBLÈMES DE SÉCURITÉ ?

O.T. En dispersant les infrastructures, le multi-cloud contribue en effet à les complexifier, ce qui accroît la difficulté d'en garder le contrôle. Les grands fournisseurs de cloud public consacrent des moyens très importants à la sécurisation de leurs services et proposent des solutions de sécurité à leurs clients. Néanmoins, il ne relève pas de leur responsabilité d'assurer le respect de conditions indispensables telles que l'hygiène des infrastructures, la gouvernance et les processus

de sécurité ou les services de proximité. C'est là que Telindus, fort de ses capacités en matière de services managés et d'intégration, a un rôle essentiel à jouer.

F.H. Parmi les Responsables de la Sécurité que je suis amené à rencontrer, beaucoup me disent ne pas savoir à quoi s'attendre avec l'avènement du multi-cloud et s'inquiètent de ne plus être capables de maîtriser toute la chaîne de sécurité de bout-en-bout. A cet égard, un acteur de confiance comme Telindus est d'autant plus précieux. En effet, en plus d'être un partenaire de proximité pour nos clients, nous entretenons depuis longtemps une relation étroite avec les grands fournisseurs de cloud public, ce qui nous donne une longueur d'avance pour protéger nos clients souhaitant faire le pas vers ce type de plateforme.

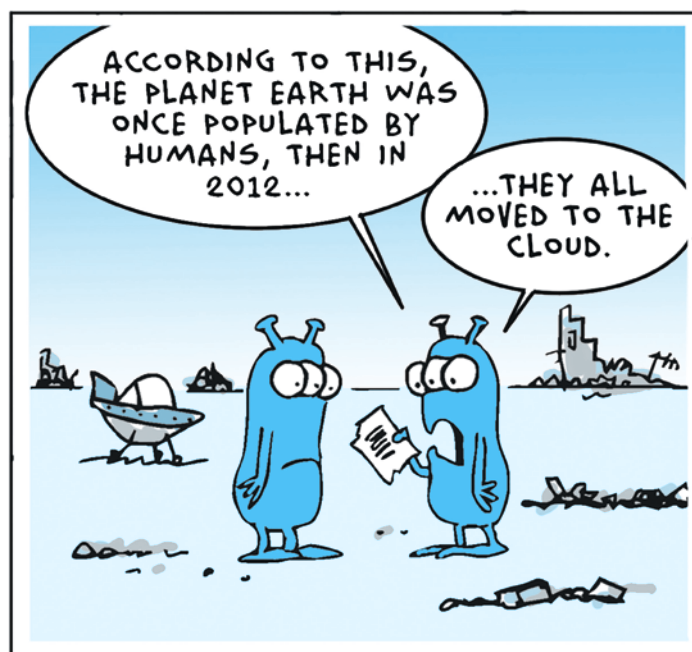
AFTER-WORD

In its first decade, cloud computing was itself a disruption, transforming businesses like no other technology. But with cloud-enabled innovations, such as artificial intelligence, the Internet of Things or blockchain, it is clear that the true extent of its impact has yet to be felt.

Organisations are under pressure to transform and innovate at the same pace as industry disruption. To achieve this, businesses need the flexibility and freedom to exploit services from multiple clouds, and to be equipped to deliver competitive, innovative and elastic applications that they can easily integrate across the enterprise.

We, Telindus, believe in a future that benefits from both on-premise and cloud resources. There is a need for both: different industries – and different organizations – will have distinct needs and considerations influencing the degree to which these options are selected. Most companies will benefit from a combination of cloud and private infrastructures – hybrid resources that offer cost efficiencies and appropriate security controls, along with optimizing compute capacity and existing IT investments.

Be that as it may, the Cloud is here to stay. It is growing daily across businesses of all sizes and has become an absolute necessity, not only for companies to remain competitive, but also as the foundation for the next wave of innovations.



Un cloud hybride Microsoft Azure intégré.

Déployez en un seul mouvement un cloud privé local qui se raccorde parfaitement aux services d'Azure public cloud.

Vos 4 avantages:



La solution la plus configurable



Une performance optimisée



Une sécurité inégalée



Tarification à l'utilisation



Plus d'informations ?

hpe.com/cloud/azure-stack

ou contactez Paul Secreti – Partner Business Manager – secreti@hpe.com



Telindus, first certified
Hybrid Cloud Integrator
in EMEA.

cloud.netapp.com

The NetApp logo features a stylized square icon on the left, followed by the word 'NetApp' in a bold, sans-serif font with a registered trademark symbol.

NetApp®

PARTNER

HYBRID CLOUD INTEGRATOR
SPECIALIZATION