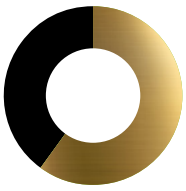
What I wish I'd known

Securing your move to – and operating in – the cloud

The route to a successful and secure cloud transformation can be a journey strewn with obstacles and potential pitfalls. Here are some top tips to smooth the way forward



60%

of organisations will use an external service provider's cloud managed service offering by 2022

Gartner 2019

More and more organisations are relying on Cloud. Recent figures show[1] that by 2022 up to 60 percent of organisations will use an external service provider's cloud managed offering. They are taking advantage of the myriad of organisational, cost, agility and productivity benefits cloud can provide.

A handful of pioneers say they have already reached cloud-only status, with the move to a virtual datacentre top of mind for many chief executives, chief financial officers, chief information officers and chief information security officers.

Our article, Managing the successful convergence of IT and OT, explored the established facts of IT and OT convergence – the known knowns, the things we know we should know, but do not – the known unknowns and the factors we're unaware we do not know – the unknown unknowns. This time we apply the same approach to cloud security.

What are the most critical elements to ensure you reap the benefits of Cloud while ensuring security and compliance?

> A handful of pioneers say they have already reached cloud-only status, with the move to a virtual datacentre top of mind for many

Known knowns

Many firms' move to Cloud has been accelerated by a need to create IT environments that can support emerging technologies, such as the internet of things, edge computing, artificial intelligence and 5G, in addition to the other benefits Cloud brings. Current momentum is such that Gartner projects the market for cloud services to grow at nearly three times the growth of overall IT services through to 2022.[2]

These figures indicate organisations are moving forward with their cloud strategies and with this a new approach to security and privacy is needed. Cloud security has been the elephant in the room, but it is now the enabler of this new shift.

Migration of traditional datacentres to a hyperscale environment, which can easily scale in line with an organisation's demands without requiring either additional capital expenditure or physical space, cooling or electrical power, introduces new issues around security, privacy and compliance for the enterprise. However, if these are addressed and managed as part of an integrated, holistic cloud strategy, then these risks can turn into rewards.

Known unknowns

What does cloud security mean in practice? Not many companies are starting from scratch in their move to Cloud, as almost all have already adopted some level of cloud usage.

This has provided an understanding of the known unknowns, for example the challenges associated with so-called cloud sprawl when it comes to migration.

Often data is fragmented across the business, perhaps stored in cloud applications already purchased and used ad hoc by individual departments, frequently without the knowledge of the CIO. This lack of strong governance in technology adoption can lead to siloed data and application islands, limiting an organisations ability to take advantage of Cloud's benefits. Many enterprises now tackle this by performing a cloud security maturity assessment and defining a unified cloud strategy based on the results.

What is cloud sprawl?

When an organisation uses several different clouds, without the central means to view, secure or manage each of them effectively, this can result in a lack of visibility and control.

An overwhelming number of enterprises are entrusting their mission-critical apps to Cloud, enabled by the options on offer from a hybrid or multicloud strategy. Currently, 62 percent of public cloud adopters are using two or more unique cloud environments/platforms and 74 percent of enterprises describe their strategy as hybrid or multicloud.[3] With the scale and speed of cloud adoption rapidly increasing, it is essential to have a unified cloud security framework that supports your overall cloud strategy.

Cloud transformation journey

As rising security threats, risks and compliance requirements become more important to businesses, we recommend that you follow these steps 01-06 (opposite) on your cloud transformation journey. These elements are not security driven, but focus on over all cloud transformation. However, security and privacy are integrated aspects that need to be considered at every step. To make this more tangible, on the following page we have highlighted three key areas to address as part of your Cloud security strategy, which will be part of the overall cloud transformation.

Firstly, we examine the importance of building a security strategy with identity at its heart. Next, we explore the emergence of DevSecOps for building modern security from the ground up. Finally, we outline how monitoring can ensure you know exactly what's going on in your cloud environment at any time. This list is not exhaustive, but highlights some of the critical challenges faced moving from traditional to cloud-based environments.

$331.2bn

of organisations will use an external service provider's cloud managed service offering by 2022

Gartner 2019

01

Baseline
Assess the current IT footprint including in-flight projects and constraints. Capture issues and opportunities and perform a security maturity assessment of the current state cloud estate.

02

Vision
Get business alignment, define guiding principles and set the pace of the journey to Cloud, including the security and privacy vision.

03

Strategic decisions
Find the right mix of public, private or hybrid cloud. Evaluate key platforms taking security and privacy aspects into account and decide on the transformation approach.

04

Organisational impact
Define the future governance and organisation, including processes, considering DevSecOps (the philosophy of integrating security practices within the DevOps process) principles. Highlight impact on talent acquisition.

05

Financial impact
Calculate the value case. Show costs, potential savings and the impact on both capital expenditure for upfront IT investments and operational expenditure, based on a subscription model for IT consumption.

06

Roadmap
Wrap up decisions of previous phases into a bought-in plan, including dependencies and key milestones.

Identity

An organisation's traditional security perimeter used to be a physical boundary. It is now a digital one. This approach is still used initially, but is no longer as effective as using business applications. IT, in general, has changed significantly; with the growth of mobility and cloud it is still just as important to protect and manage sensitive data outside the confines of an organisation. Indeed, it is estimated that a quarter of all breaches in 2020 will happen outside the traditional security perimeter.[4]

With Cloud enabling a new generation of employees who can work from anywhere, across any device, creating the waves of data flowing freely, we need to define a new perimeter of identity and access management.

Cloud security strategy must be based on credentials: who is the employee, partner or contractor and what access are they allowed to particular data and services, under which conditions and from where? For example, identification to access data might be different if it is done from country "x" compared to country "y".

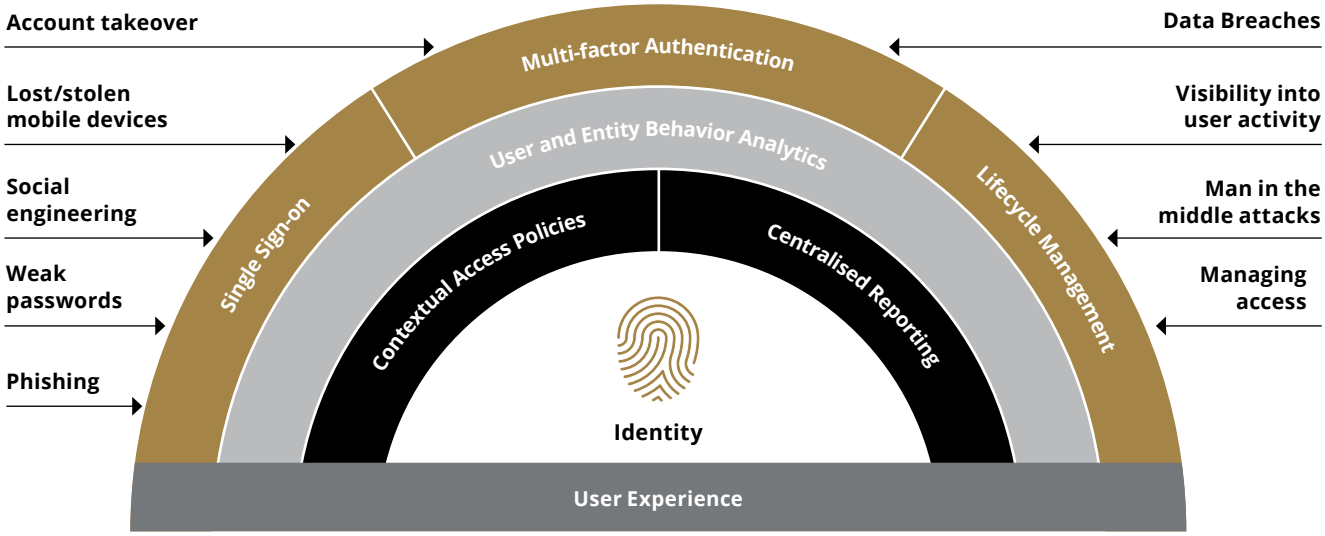
An organisation might also consider adopting per-application access controls for contractors or setting clearer restrictions around what data is available to all employees. From a cloud security perspective, getting identity and access management right is crucial and needs to be a central element in every cloud transformation.

DevSecOps

In the cloud environment, organisations need stronger collaboration between the development, security and operational functions to develop business applications more rapidly or have a more agile way to extend their IT infrastructure.

It is where we see the convergence of the traditional security team with the software development and the IT operations team within an organisation. The initial concept was

The new enterprise security model



Secure
Securely prevent phishing, social engineering, and data breaches while enabling seamless access to cloud and mobile apps

Vigilant
Vigilant detect unusual behavior while respecting user privacy and keeping alert volumes manageable

Resilient
Resilient in response to possible attacks through adaptive access and alerting across both On-Premise and cloud apps

called DevOps and is now extended to include security and privacy at its core with DevSecOps.

Incorporating culture, practices and collaboration, DevSecOps leverages the best of all worlds. It sees the security, development and operations teams working together holistically to ensure security is embedded from the very beginning, and into each phase, of the DevSecOps pipeline.

This may be no easy task initially[5] and will be as much a cultural issue as a technical challenge. Some employees may be reluctant to embrace the new way of working, which means business leaders may need to educate them to instil this mentality throughout the organisation.

The main challenge is to ensure all stakeholders adapt to the new approach and work together. It is important to establish foundational DevSecOps governance in the early stages to provide a roadmap to transform people, processes and technology.

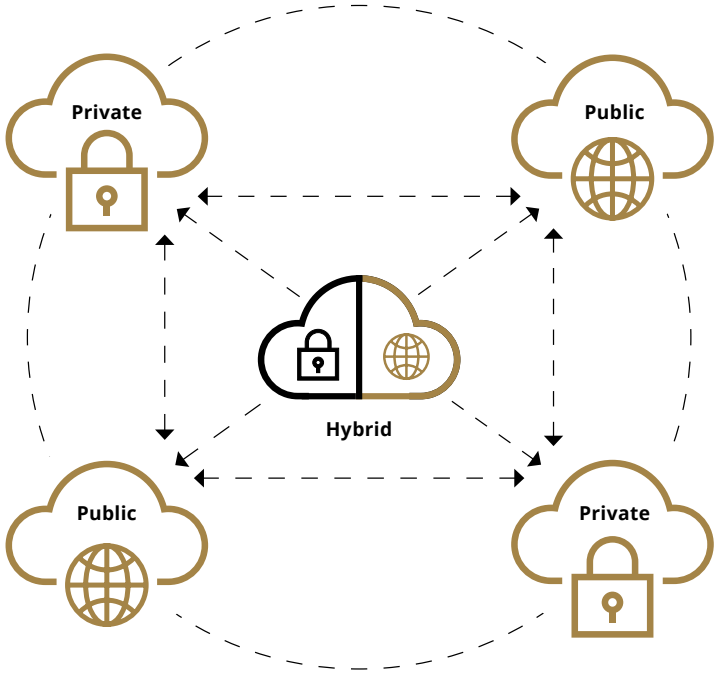
Cloud security and compliance monitoring

Another key area is to establish continuous, proactive monitoring of the cloud environment to ensure security and compliance controls are being adhered to. This will enable detection of possible intrusions, as well as security and compliance policy violations, and ensure a quick response to any threats and compliance breaches.

Also, it may sound obvious, but don't just trust that everything deployed in Cloud is performing as expected. The good news is it's possible to achieve the same level of familiarity, visibility and control over a cloud environment as with on-premise infrastructure.

Continuous cloud monitoring will not only help detect cyberthreats, but will also enable clear sight of all workloads migrated to Cloud, to monitor whether they are running as they should on a day-to-day basis, ensuring optimum cost-efficiency, and that they fulfil all security, privacy and compliance requirements.

Multicloud, Hybrid Cloud



Your unknown unknowns

Cloud has become an omnipresent topic for businesses and is changing the face of the IT landscape across every industry. Businesses are now spending more on cloud infrastructure[6] than they are on on-premise infrastructure, with the gap set to widen significantly over the coming years as organisations ramp up their investments in next-generation technologies and move to virtual datacentres.

Hyperscale cloud providers implement innovation at a rapid pace, and potential opportunities, but also challenges, change rapidly and constantly. The move to cloud is a multi-step journey and strategy. It is important to put security and compliance at the core of the planning process from the beginning and keep it as an integrated aspect throughout the whole innovation, migration and operations process.

As with many unknowns, the move to a virtual datacentre and hyperscale global networking, sees many organisations try to reinvent their IT strategy. They expect not just IT operations, but also security and privacy, to adapt rapidly to this new way of digitalisation to keep information and systems compliant, secure and available.

As a CIO, CISO, CFO or even CEO, you need to see a return on investment in cloud. Follow the steps outlined here and your organisation will reap the most benefits from your cloud migration. ■

Reto Haeni
Partner, Swiss Risk Advisory,
European Cloud Security lead

rhaeni@deloitte.ch

Endnotes

1. https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020
2. https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g
3. https://medium.com/@jaychapel/multi-cloud-hybrid-cloud-and-cloud-spend-statistics-on-cloud-computing-ba4c194d2e10 https://www.watchguard.com/wgrd-resource-center/predictions-2020%23perimeter
4. https://www.watchguard.com/wgrd-resource-center/predictions-2020%23perimeter
5. https://www.tanium.com/press_releases/tanium-study-strained-relationships-between-security-and-it-ops-teams-leave-businesses-at-risk/
6. https://www.cloudindustryforum.org/content/cloud-infrastructure-spend-surpasses-spend-legacy-it-finds-new-research-cif

Deloitte.