Securing the hybrid cloud

We live in a digital era where born-digital organizations such as Uber, Airbnb and Netflix are disrupting entire industries. These rapid changes are forcing organizations to innovate more aggressively and become more agile in response to ever changing market demands and global consumer trends.

CEOs, in turn, are looking to their CIOs to develop and accelerate their digital transformation strategy, one that will allow them to adapt to current trends and deliver against future needs.

Contents

Key cloud values

As the demands that consumers and other users place on the IT team increase, the number of companies looking towards to the cloud to provide a platform for digital transformation is increasing.

Cloud services have become a key platform in enabling transformation strategies for many organizations, as they introduce several key capabilities:

Consumptive and agile – the ability to pay only for what you use and grow and shrink as required drives an agile approach, which reduces expenses and shortens the time needed to take new services to market.

On-demand and elastic – cloud services are always available, and don't require that you extend your local data center footprint or go through long and expensive procurement cycles.

Automation – enterprises and individual buyers have the ability to provision new services and digital assets with no human interaction, and without enduring the long and exhaustive processes required to stand these up from scratch.

While agility brings speed and assures quality of service, cloud adoption has been limited to specific industries and early adopters. The early promise of cloud services did not meet initial predictions because of the risk that was assumed by the CIO, CISO, and risk committees. Organizations soon realized they were unable to use previously developed security principles and controls in public cloud environments and concerns have risen about the potential for data loss and reputational damages. Resource pooling and shared platforms are the building blocks of public cloud, but the transition of enterprise applications to this model has been delayed as a result of the security. Private cloud offers dedicated resources and enhanced security controls, yet at the same time loses some of the elasticity and agility of public cloud services. These services have evolved over time to meet the growing demands of organizations and now include packaged offerings known as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-or Application-as-a- Service (SaaS). Hybrid cloud is known as the combination of two or more cloud platforms as depicted in the below diagram. Secure hybrid IT is the practice of enforcing already developed security principles and strategies, regardless of where the services are hosted.

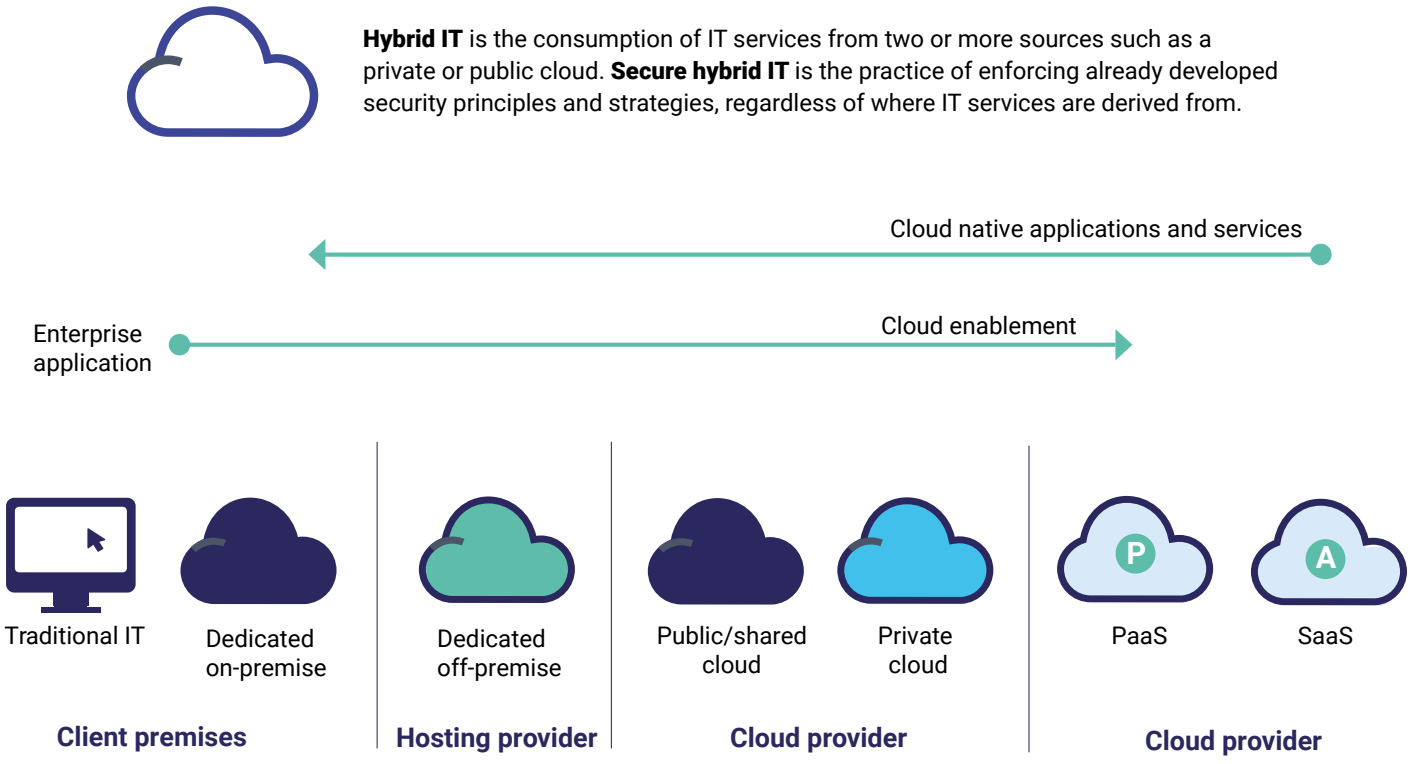

Figure 1: Cloud evolution overview

Ensuring the viability and security of applications is a fundamental requirement in the transition of traditional resources to a cloud platform. Using the disciplines and technologies developed over the years to protect the local data center soon became cost-prohibitive and limited in terms of both scalability and elasticity. As such, it was not suitable for the evolving world of hybrid IT. To cater for this, we introduced a secure hybrid IT packaged offering, to help clients accelerate their cloud transformation journey by ensuring the security of cloud applications and respective peripheral infrastructure components. Secure hybrid IT is based on a holistic 'defence in depth' approach designed to secure each and every layer and ensure the availability of applications and the integrity of information. This approach includes the following key modules:

1. **Illuminating** the network to discover all assets, regardless of operating system, location or specific use. This is key to ensuring that appropriate access to network resources is managed in a coherent and risk-driven manner.
2. **Compartmentalizing** the distinct services and service elements to force physical and logical separation on the basis of trust. This includes physical and logical (micro and nano) network segmentation, in line with current service- oriented architecture methodologies and best practice.
3. **Inspecting and analysing** every piece of information by employing real-time smart capture and advanced analytics techniques. This is key to forming a consistent and scalable framework for protecting applications on all layers.
4. **Consolidating** network and compute resources to accelerate the vision of a converged, highly-scalable, cost-effective, and secure network. This ensures the viability of a cloud strategy as the network becomes fuel for cloud services. Regional offices, remote users, overseas consumers, and corporate IT employees are all the beneficiaries of this network-as-a-platform concept which drives a consistent and cost-effective user experience.
5. **Continuous evaluation** of risk posture, compliance status and overall security performance. This can drive a repeatable approach, through the use of predeveloped security profiles which reflect the organization's needs, its risk appetite, and reinforces best practices.

Overall, adopting a cloud strategy is far more than a lift-and-shift exercise where local workloads are transitioned to a cloud platform. It requires revisiting the entire architecture and re-evaluating fundamental ideas that may have been around for years. This re-evaluation is critical in order to change the architecture into something that both reflects current needs and introduces the concept of a service-oriented architecture. It also demands investment in the new skills required for this new hybrid cloud era, such as a cloud architect, cloud data scientist and cloud application specialist.

The potential of cloud is enormous. It nourishes the rapidly growing digital economy. However, security and privacy are two fundamental concerns that organizations considering transitioning of legacy applications to the cloud have.

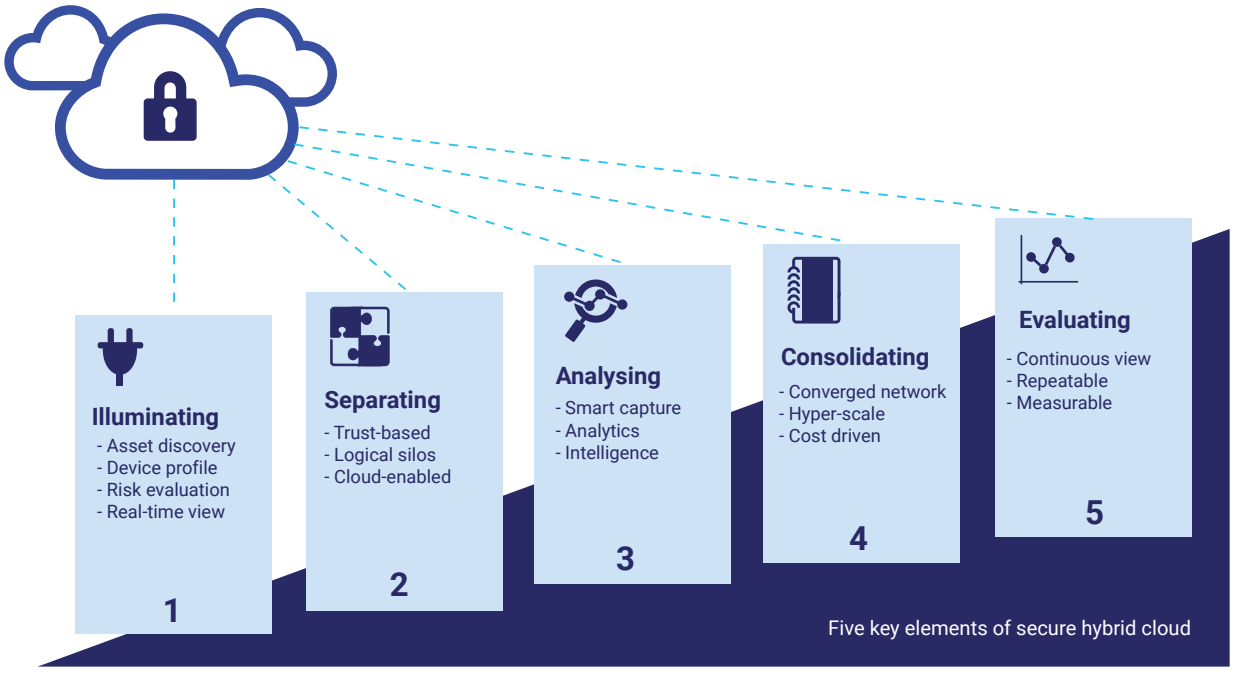

Figure 2: The five key elements of secure hybrid cloud

Securing the cloud: Who is responsible?

Make no mistake, hybrid cloud is coming. Even though it's increasingly identified as the preferred model by IT teams - with the explosion in cloud offerings - responsibilities are blurring. Traditional IT involves the enterprise taking accountability for physically and logically securing applications, but this model blurs somewhat as we move into offerings such as IaaS. These new responsibilities require careful mapping into a cloud responsibility matrix.

The below diagram is an example of a matrix offered by the Cloud Security Alliance and can be used as a reference. This matrix needs to reflect the organizational IT footprint and agreed responsibilities, in line with any relevant service-level agreements.

These new responsibilities require careful mapping into a cloud responsibility matrix. **The below diagram is an example of a matrix offered by the** Cloud Security Alliance **and can be used as a reference**

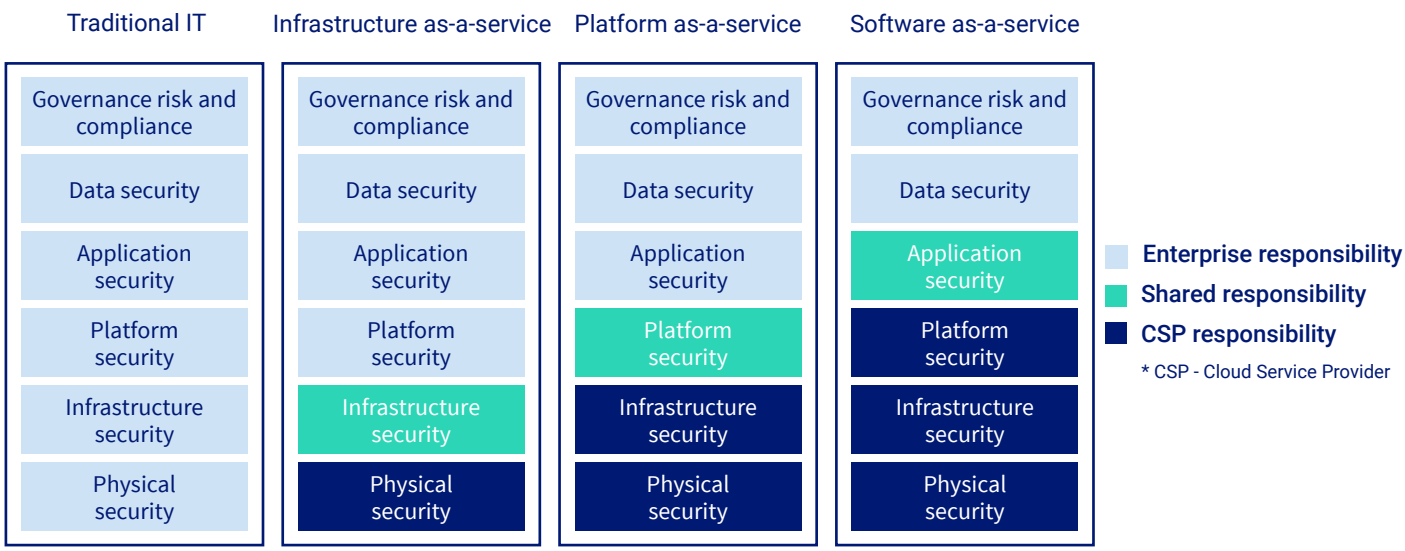

Figure 3: Cloud security responsibility matrix. Source: Cloud Security Alliance

Identity and access

As organizations extend their digital footprint into the cloud, identity and access is becoming a key catalyst in setting the overall pace of cloud adoption. Traditional user repositories, such as Active Directory, LDAP and RADIUS have morphed into cloud offerings supporting the transition of enterprise applications. Recent examples include Microsoft's Azure Active Directory and Amazon's directory services. As hybrid cloud is adopted more widely, a further extension to this approach will be required to support user identities and application access in a heterogeneous environment. The world of hybrid cloud requires a federated and decentralized approach that can meet an organisation's needs to authenticate, identify and authorize access to critical assets across on-premise, off-premise and on various cloud platforms. This approach needs to support multiple cloud platforms, include native identity management tools and offer a clear migration path for applications that are transitioned into the cloud. This is known as the Cloud Identity and Access Management (CIAM) framework.

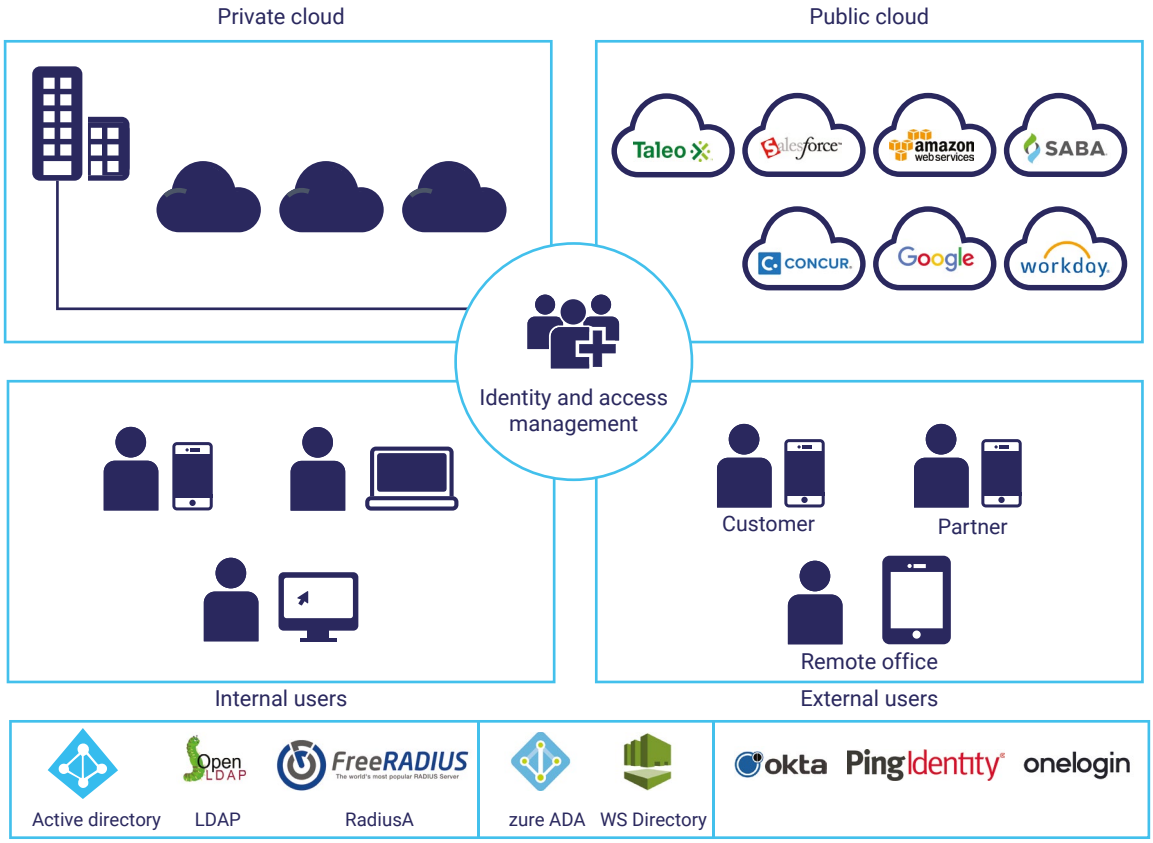

Figure 3: Cloud Identity and access management framework

Compliance and regulation

Cloud platforms have an appealing image, but when it comes to compliance, things may not be as simple as they seem. As platforms mature and evolve, governments and regulatory bodies are tightening regulatory and compliance requirements. Compliance provides the service provider with a rubber stamp, in terms of their alignment with security, privacy, and operational best practices. Ensuring adherence, compliance or conformity with regulatory requirements can be challenging with traditional on-premise environments, but with cloud services it's even more so. Organizations with an international IT footprint might end up with conflicts between the legal requirements of different countries and will require clear mapping and thorough analysis of the relevant compliance requirements. Examples of some common regulations include:

- **General governance** – ISO/IEC 38500, ITIL, COBIT, NIST, SSAE-16, ISO/IEC 90001
- **Security best practice** – ISO27001, SAS-70 Type I & II, NIST 800-53, SOX
- **Data privacy** – AU Privacy Act 1988, EU General Data Protection Regulation, US Privacy Shield
- **Industry specific** – PCI-DSS (payment Industry), HIPAA (Healthcare)
- **Audit and reporting** – SSEA-16, SOC-2, SOC-3

According to a recent 451 Research report, compliance-related concerns are a significant barrier to cloud adoption. The recent EU General Data Protection Regulation has taken this a step further to include penalties of up to 5% of an offending organization's global turnover. A few key guidelines that can assist organizations in driving a sustainable approach are:

- know where your cloud applications are processing and storing information
- classify data and take measures to protect personal data from leakage, theft or alteration
- restrict access to systems to avoid any unauthorized access
- collect only 'necessary' information and don't use personal information for other purposes

Secure hybrid cloud – key service elements

Visibility, across the physical and logical digital estates, is key to maintaining a current asset register, ensuing a compliant state, and managing the overall risk posture. We offer real-time network illumination to allow organizations to keep track of all network entities and to drive an efficient network access strategy.

Network segmentation is one of the most effective measures in limiting threats and any potential lateral movement. To support segmentation in current cloud environments, including the recent addition of Docker technology, we offer an elastic and hierarchical approach, supporting micro- and nano-segmentation techniques for complete service compartmentalization.

Traditional controls have evolved over the years into what we now refer to as next- generation technologies. This was deemed fit for some time, but does not reflect the current need to support hyperscale and extremely elastic environments. We offer a revolutionary approach supporting advanced analytics and controls, built into the core of the cloud. This allows us to scale the digital footprint vertically and horizontally with no need to change any architectural concepts or application development processes.

As the organization scales into the cloud, the network is becoming the glue that provides scalability, elasticity and responsiveness. Wide area network costs are rising exponentially and this does not work well with the new cloud model. We offer application-driven connectivity controls to drive elastic application-centric access policy controls.

Automation is a key component as part of every cloud strategy. This is vital in driving the required elasticity and reducing the need for human involvement and operational overheads. We offer an advanced services layer which allows clients to automate provisioning, migration and monitoring processes via robust APIs and our client portal.

As perimeter borders blur, the threat surface expands and the endpoint has become the new frontier. We offer a set of advanced tools for server and endpoint protection. This is key to identifying and mitigating advanced threats and ensuring the integrity and livelihood for key services. It's also vital to the extraction of advanced analytical intelligence, which can be used to identify any fraudulent or non-compliant activities.

As applications evolve into the cloud, the traditional-centric architecture is becoming obsolete. This is slowly morphing into a distributed and stretched architecture where frontend, middleware and backend, may all be hosted at different locations and on different digital platforms. This calls for an application-centric policy, that will be agnostic to physical location or hosting platform and have the required elasticity to stretch in either direction.

Continuous monitoring of compliance status and overall security posture remains vital for all organizations.

With new services and a growing number of changes, ensuring compliance and alignment with a baseline state is critical. This can be monitored across a set of common metrics and vendor mappings to follow common taxonomy and to drive a consistent compliance baseline.

Conclusion

For almost every company the move from a traditional IT to a hybrid IT environment is already underway. However, there are numerous pitfalls as issues around security, compliance and regulation come to the fore. None of these should prove insurmountable in the drive to unlock the efficiencies of cloud services, but all need to be actively managed to ensure they do not result in difficulties further down the road.

Disclaimer: The work described in this whitepaper was performed while the company was known as Dimension Data.


NTT