Securely enabling cloud adoption.

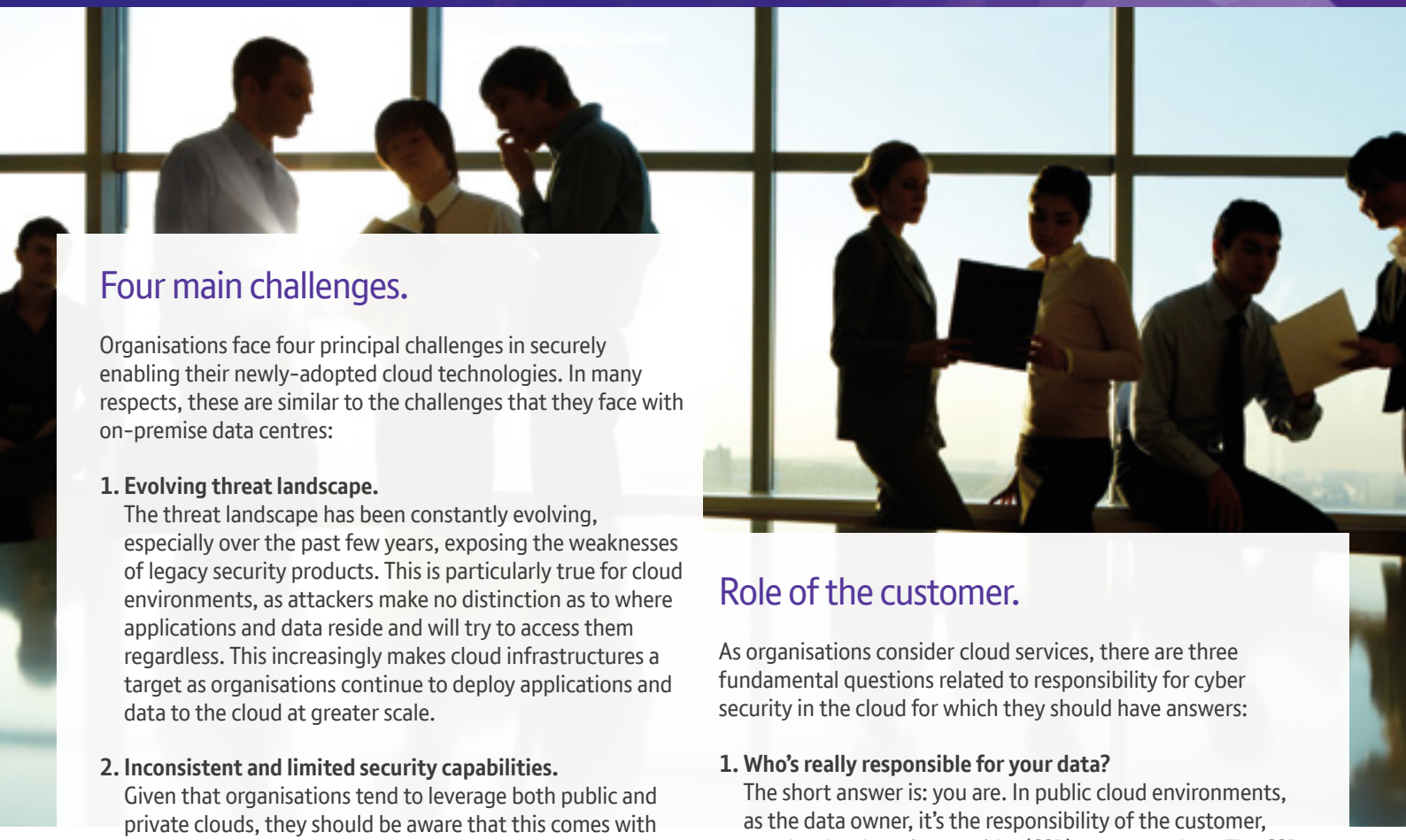
Our expertise. Your priorities. World-leading cloud security.

The demand for organisations to be more agile to meet customer needs and stay competitive is driving a change in the way applications are developed, deployed and adopted. As organisations increasingly take advantage of virtualisation by adopting the cloud, their applications and data become more distributed, thereby expanding potential avenues for compromise. When networks span on-premise, physical data centres, as well as public and private cloud environments, simply ensuring an accurate view of your security risks is a considerable endeavour.

The benefits of moving to the cloud are well-documented, relating to both increased organisational agility and lower costs associated with reduced capital and operating expenses. The challenge now is how to meet the agility needs of the business, while protecting applications and data deployed in the cloud without adding complexity or cost. Organisations need a prevention-focused security architecture for cloud deployments that stops threats across all potential attack vectors.

The goal of this paper is to help guide organisations through the security considerations associated with moving to the cloud. By highlighting some key questions to ask and rules to follow when articulating a cloud strategy, this paper will help organisations take advantage of the cloud with the confidence that they're not leaving themselves exposed to new cyber security risks.

paloalto NETWORKS | BT



Four main challenges.

Organisations face four principal challenges in securely enabling their newly-adopted cloud technologies. In many respects, these are similar to the challenges that they face with on-premise data centres:

1. **Evolving threat landscape.**
   The threat landscape has been constantly evolving, especially over the past few years, exposing the weaknesses of legacy security products. This is particularly true for cloud environments, as attackers make no distinction as to where applications and data reside and will try to access them regardless. This increasingly makes cloud infrastructures a target as organisations continue to deploy applications and data to the cloud at greater scale.

2. **Inconsistent and limited security capabilities.**
   Given that organisations tend to leverage both public and private clouds, they should be aware that this comes with differing security capabilities offered by differing cloud partners. This, coupled with the use of individual security products geared towards a specific kind of cloud, can quickly lead to inconsistent security postures, leaving applications and data exposed.

3. **Manual security operations.**
   Reliance on manual security operations cannot keep pace with business needs in public, private, and hybrid cloud environments. Workloads in cloud environments get spun up and spun down at very high rates and can have a lifespan of months, days, hours, or even minutes. Relying on manual operations to apply security policy in this context is untenable and greatly increases the probability of workloads becoming compromised before policy is applied.

4. **Decentralised management.**
   As organisations adopt multiple cloud technologies, relying on decentralised security policy management has become a serious challenge. While there may be legitimate business reasons for adopting multiple cloud technologies, enforcing a uniform security policy can be an onerous task, given the differences in the underlying infrastructures.

By addressing these four challenges, organisations will be better positioned to securely enable their cloud adoption and take advantage of the agility promised by the cloud. Before taking these challenges on, however, organisations should clearly understand their role in cloud security.

Role of the customer.

As organisations consider cloud services, there are three fundamental questions related to responsibility for cyber security in the cloud for which they should have answers:

1. **Who's really responsible for your data?**
   The short answer is: you are. In public cloud environments, as the data owner, it's the responsibility of the customer, not the cloud service provider (CSP), to secure data. The CSP secures the underlying cloud infrastructure, but customers are responsible for the security of their applications and data. Organisations must therefore ensure that they're able to deploy a consistent security posture, regardless of where their applications and data reside – whether on-premise or in the cloud.

2. **Who has access to your applications and data?**
   Clearly defining role-based access policy can help mitigate the risk of data loss as a result of either malicious activity or inadvertent disclosure. While the CSP will have authentication and authorisation methods in place, there are some fundamental choices to make – like who should have access and if additional assurance, such as multifactor authentication, is required. Establishing this between the customer and CSP is a crucial first step to managing cloud security risks.

3. **What happens if there's a security breach?**
   Organisations must understand what kind of support they'll receive from their CSP in the case of a breach, and do so ahead of time. Mid-response is not the optimal time to discover who's responsible for what.

Armed with answers to these questions, executives will be well placed to fulfill their risk management duties to their organisations, and direct investment to reduce cyber risk accordingly.

Achieving key security imperatives.

As organisations articulate their cloud strategies, there are four imperatives for securely enabling cloud adoption that they should bear in mind as they select CSP and cyber security partners:

1. **Gain visibility of all traffic.**
   In order to prevent attacks, organisations must have application, user and content-level visibility of all the internal and external traffic transiting all their environments, including the cloud. It's impossible to secure what's out of sight, and having this visibility is a crucial first step in enabling a risk-based security posture.

2. **Establish a consistent security posture.**
   Preventing successful attacks requires consistent protection of applications and data, regardless of how or where users access them. Organisations must therefore have a unified security posture composed of natively-integrated components to protect applications, users and data from both known and unknown threats. This establishes a logical security perimeter that protects applications and data, regardless of location – ensuring that public and private environments have the same level of protection as the on-premise data centre.

3. **Centralise security management.**
   As organisations adopt multiple cloud technologies, relying on decentralised security policy management can introduce additional complexity that leads to an inconsistent security posture – potentially leaving applications and data unprotected. Organisations must therefore have centralised policy management that allows for configuration of policy in one place for application across all clouds.

4. **Automate security to enable agility.**
   To deliver on the promise of the cloud, security must keep pace with business workloads by using automated deployment and policy updates. This enables the elasticity of the cloud by requiring the deployment of applications and security in lockstep, which improves security posture and reduces administrative effort.

With partnerships in place to deliver these outcomes, organisations will be properly positioned to take advantage of the agility of the cloud, while effectively managing the associated new security risks.

Case study: Virtual desktop infrastructure.

Business driver: A multinational financial services institution, seeking to act with greater agility and save costs in an increasingly competitive environment, wants to virtualise the desktop infrastructure for its new and existing branch locations.

Security challenge: Provision and de-provision branch virtual desktop infrastructure (VDI) with a consistent security posture to enforce role-based access to applications, ensuring that only the right employees have access to the applications they need to do their jobs.

In order to overcome this challenge, this financial services institution would need to address the four aforementioned security imperatives:

1. **Gain visibility into all traffic.**
   The first step to securing branch VDI would be to deploy technology to gain full visibility of traffic to and from its cloud resources, mapping all traffic to specific applications and user identities. This will allow for the creation of a list of approved applications, such as those the virtual desktop application branch offices rely on to operate, setting the bank up for secure enablement.

2. **Establish a consistent security posture.**
   With this full visibility, this bank is positioned to protect its cloud environments from attacks. By putting into place a logical security perimeter that protects applications and data, regardless of location, cloud environments will have the same level of protection as the on-premise data centre. In this example, this may mean putting the virtual desktop application in a private cloud, and enforcing role-based access to that application. This ensures that only the right employees have access to the applications they need to do their jobs.

3. **Centralise security management and automate security.**
   By establishing a consistent and unified security posture, this bank can now spin up new workloads, like additional virtual desktop instances for new branches, with security policy deployed in tandem, automatically.

By addressing the security imperatives, this financial services institution will be able to achieve this cloud-based project with security built into its operations, allowing it to respond to competitive pressures and new opportunities with greater agility.

Conclusion.

The adoption of new technologies that unlock organisational agility must be securely enabled without the introduction of additional complexity or prohibitive costs. Organisations seeking to embrace cloud computing must take into consideration four primary challenges in order to do so securely. A rapidly evolving threat landscape now includes cloud infrastructures, as adversaries will target applications and data, regardless of where they reside. Additionally, as organisations adopt different cloud deployment models for different parts of their operations, they expose themselves to the inconsistent security capabilities of their CSPs and the limited capabilities of point products specially designed for one kind of cloud, which can lead to an inconsistent security posture, leaving applications and data vulnerable. Finally, reliance on manual operations and decentralised management to provision security cannot keep pace with cloud workloads, which increases the probability of compromise.

While these challenges may seem barriers to securely enabling cloud adoption, they are surmountable with the right approach. First, organisations must recognise and embrace their responsibility as data owners for the security of their applications and data in cloud environments. With this mindset established, organisations must have security technology that provides full visibility of all traffic transiting cloud environments, and then contextualise this traffic to specific applications and user identities. With this visibility, organisations will be in a position to establish consistent security postures, protecting applications and data anywhere their users access them. Security policy must be centrally managed in order to configure policy in one place and then deploy to all environments, and organisations must be able to automate the deployment of security to move at the speed of business needs.

By addressing these security imperatives with the right approach, organisations will be well positioned to meet the need for agility to meet customer needs, take advantage of new opportunities and respond to competitive pressures.

Find out more: go.paloaltonetworks.com/happycloud | bt.com/security

October 2016