PROACT

#ThePowerOfData | #ThePowerOfTogether

WHITEPAPER

Developing a hybrid cloud security strategy

Consistent protection in a hybrid cloud environment

Contents

Abstract

Organisations are increasingly adopting hybrid cloud due to the multitude of benefits this architecture type offers. Concurrently, the integral role of consistent security throughout all aspects of an IT environment is quickly becoming more apparent against the backdrop of an increase in cybercrime.

Due to its deconsolidated nature, a hybrid cloud architecture presents unique complexities in terms of both visibility and consistency when it comes to security. This white paper discusses the security challenges of a hybrid environment and presents solutions to develop a hybrid cloud security strategy with reliable protection in mind.

Introduction

Please note that the term "hybrid cloud" is used throughout this paper as it is defined by Gartner and IDC: A solution using multiple deployment models.

The use of hybrid cloud architectures – wherein an organisation combines several different deployment models, such as on-premises infrastructure, private clouds, managed clouds and public clouds – has surged within the past several years. In fact, as of 2021, 76% of enterprise organisations have adopted a hybrid cloud strategy.[1]

The popularity of hybrid cloud can be attributed to its ability to enable organisations to gain advantages in speed and flexibility. Furthermore, it can drive business value by leveraging cloud-native functionalities, like low/no-code functions, PaaS and SaaS services.

Talk to us about driving growth and automation with a secure hybrid cloud solution.

Despite the numerous advantages offered by hybrid cloud adoption, there are aspects of this architecture type that have the potential to increase complexity. Most significant here is the issue of security, as the deconsolidated nature of hybrid cloud creates a broader surface from which attacks can enter an environment.

This broader surface also often results in decreased visibility of the individual components within the environment from a security standpoint. Furthermore, security consistency between clouds and across an environment can create a challenge when the measures used within an organisation internally can't be applied to a cloud vendor. When frequently changing compliance regulations are factored into the mix, there's even more to consider.

The simple fact is, it's all too easy to get caught up in making use of all the benefits offered by a hybrid cloud setup and inadvertently let security and compliance slide onto the back burner. However, with the right information at hand, knowing what's essential for hybrid cloud security and how to put this in place doesn't need to be overwhelming.

This white paper discusses the main security aspects to be considered in a hybrid cloud environment as well as the challenges often encountered here. Then, measures – in the form of frameworks, tools and workflows – are highlighted which can be taken to enable you to mitigate threats while making the most of hybrid cloud.

[1] *https://www.hashicorp.com/state-of-the-cloud*

Points to consider

Shared responsibility model

For organisations whose hybrid cloud infrastructure is comprised at least partially of public cloud resources, understanding the concept of shared responsibility is essential. Shared responsibility means that the public cloud provider secures their own cloud (e.g., they will ensure the physical security of their data centre(s)). The exact components protected by the cloud provider varies depending on the provider.

In contrast, whatever customers run or store within the public cloud is their own responsibility. Therefore, endpoint protection, network security, access management and data accountability all need to be managed by the customer.

With security responsibilities divided this way, statistics reveal that the overwhelming majority of security failures involving public cloud are found to be the fault of the customer rather than the cloud provider.[2] It's therefore all the more essential to put the correct measures in place for the portions of this model that an organisation itself is responsible for.

Governance/compliance

Although security responsibilities are shared between cloud providers and their customers, ensuring compliance and governance lies solely with the customer.

The first step for an organisation is to research whether it is affected by industry- and country-specific compliance regulations. These (in addition to the standard regulations such as ISO or GDPR) should then be taken into account while mapping out a strategy for how to accommodate them within a cloud environment.

The challenge with maintaining compliance is twofold: regulations and standards change frequently, so if an organisation doesn't have a role which is dedicated to keeping track of developments, it can be tedious to stay on top of the latest changes. Additionally, without the proper tools in place it is often necessary to manually analyse and report whether infrastructure complies with the latest policies. This process takes time and can be prone to error.

Want to learn more about the role of compliance in hybrid cloud? **Get expert insights here.**

[2] https://www.gartner.com/smarterwithgartner/is-the-cloud-secure

Centralised security orchestration

Many of the challenges presented by both the shared responsibility model and governance/compliance can be addressed through consolidated security operations and security monitoring. A centralised security orchestration enables visibility over the entire infrastructure regardless of cloud type. Therefore, it ensures compliance standards are met without requiring a human to constantly monitor (and implement solutions for) the latest developments.

This solution can allow the visibility that is so absolutely essential to maintain across clouds. For a hybrid cloud environment, there are several additional requirements that need to be considered:

- Tools must be scalable in order to accommodate a growing architecture and to be capable of inspecting cloud-native, PaaS and SaaS functionalities.
- New components of the infrastructure must be monitored immediately alongside the rest of the environment. It is essential to monitor every layer of the infrastructure.

The fragmented nature of a hybrid cloud environment – coupled with an often piecemeal-approach to cloud security in general – results in many organisations having a collection of different tools at their disposal. To successfully implement truly centralised security orchestration, it's vital to take stock of what technologies can be applied to a hybrid cloud environment and which can't.

To avoid clutter, it can be useful to remove those technologies which are no longer serve the new environment. At this point, it's also a good idea to assess current general security measures within an organisation and examine to what extent these cover the entire environment and where there may be gaps, or even new solutions required. Additionally, if there are still too many tools floating around that do not cover all the environment's components, a completely new cloud security strategy may be worth pursuing.

Complex but possible: Meeting the challenges

The previous sections have highlighted the main points of consideration for hybrid cloud security. While some challenges were identified, these have solutions which can be realistically and effectively implemented. Read on for recommendations about how to put them into practice.

Implementation of security operations

As discussed above, the proper implementation of a centralised security solution allows for a holistic view of what is occurring within the entire environment. This solution should encompass automation, analytics and monitoring. In combination, these elements allow an organisation to standardise security measures across clouds throughout the environment. Optimising the security monitoring solution to one that consolidates all relevant output regarding different clouds allows this information to be accessed from one location.

Enabling collaboration

One way to ensure that security remains a priority from the very beginning is to implement a DevSecOps approach. Defined by Red Hat as "[...] an approach to culture, automation, and platform design that integrates security as a shared responsibility throughout the entire IT lifecycle,"[3] DevSecOps increases protection by facilitating cooperation between development, security and operations teams, thus making security a core element of application and infrastructure deployment from the start. The collaboration involved here also makes an organisation more agile and better able to keep up with the speed of change in public clouds.

Frequently, a primary motivator for including public cloud in an organisation's infrastructure is the ability to automate processes. It is sensible to apply the principle of automation to security as well. Alongside the obvious changes in workflows it brings about, DevSecOps also introduces automation of security measures. This makes it easier to include security at the beginning of a development cycle. It can also significantly reduce the number of errors or oversights encountered in manual operations and increases visibility across the environment.

[3] *https://www.redhat.com/en/topics/devops/what-is-devsecops*

Selecting applicable frameworks and principles

Collaboration as outlined by the DevSecOps approach is first enabled when everyone has the same goals to work towards. This is made possible by selecting the correct framework and principles. There are many well-known ones to choose from which place emphasis on security.

Among them are:

Microsoft

The Zero-Trust principle

aws

Cloud Adoption Framework

NIST

Cybersecurity Framework

Microsoft

Cloud Adoption Framework for Azure

While each presents a different structure in terms of the phases and steps involved, they all cover the most important security aspects to keep in mind. Additionally, all provide a standardised approach to addressing this aspect of a hybrid cloud environment within a DevSecOps team.

In cases where the architecture consists of more than one public cloud, it is crucial to recognise that a common framework should be established that is applicable to all clouds within the environment. This can be difficult to put into practice because public cloud providers often have environment-specific architectures that make "one size fits all" solutions impractical.

It can be tempting at this stage to select a framework prioritising the business requirements of the company. Alternatively, a framework favouring one cloud provider in its design may look attractive if that is the organisation's current provider. However, with multiple (planned) public clouds, this is a recipe for both increased stress and additional costs. The same caution can be applied to situations where tools and technologies for on-premises data centres are adapted by organisations for use in the cloud — it is vital to recognise that cloud security has its own concerns which must be addressed.

Wondering which framework is right for you? **We're here to advise you.**

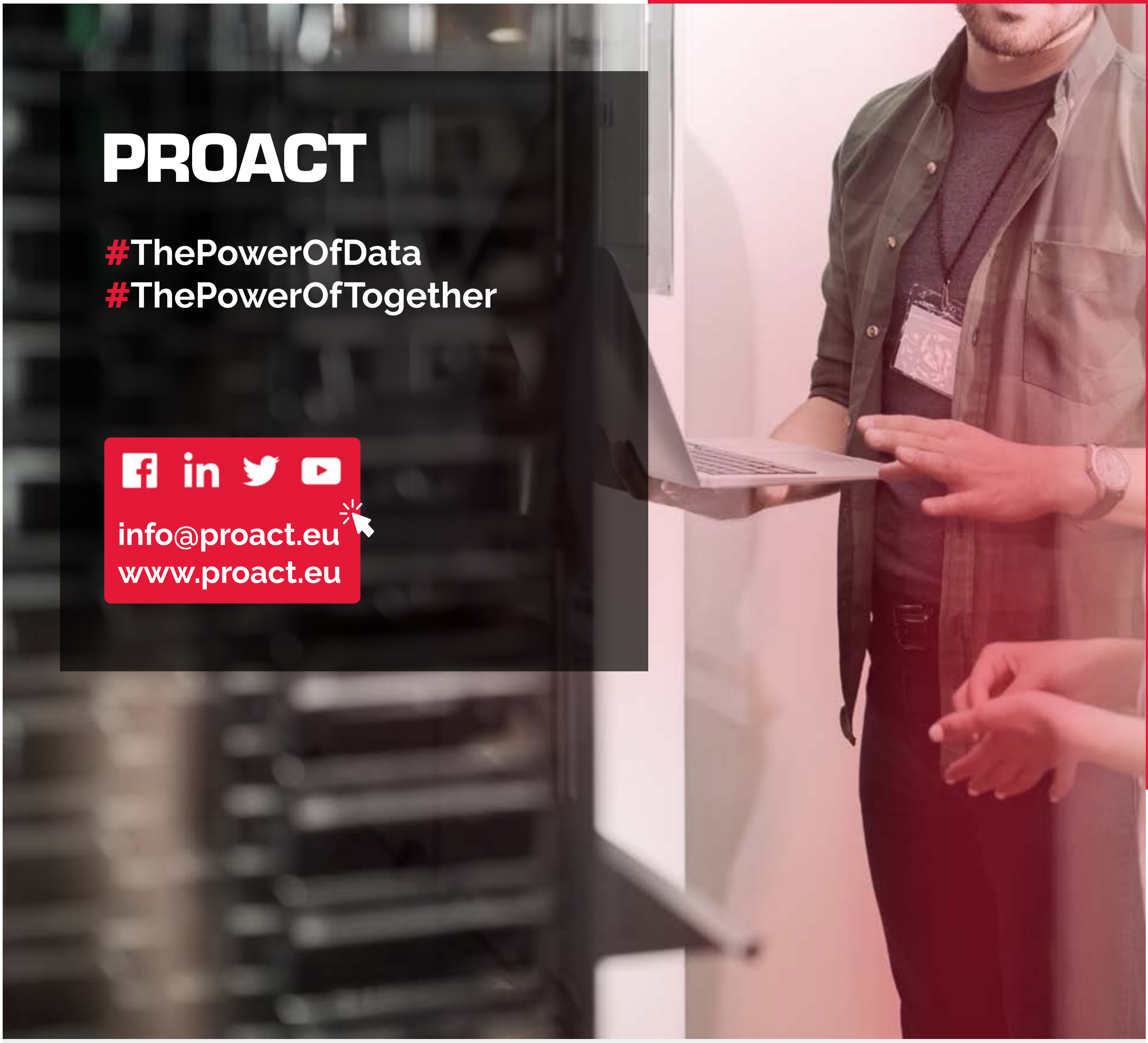
What's next?

Hybrid cloud is increasingly becoming indispensable for many enterprises. Given how integral this architecture type has become to many organisations' IT strategies, the importance of hybrid cloud security is hard to overstate. However, this setup inevitably presents a certain level of complexity due to its basic nature. Concurrently, cyberattacks are on the rise, driven by increased internet traffic caused by the Covid-19 pandemic as well as cryptocurrency enabling the anonymity of cybercriminals.

Therefore, it's more important than ever to identify what a hybrid cloud security strategy should encompass, what challenges may arise and how to address these in order to ensure that the environment has a cohesive security architecture. By not doing so, organisations inadvertently can put themselves and their data at risk for attack.

Security and compliance are best seen as moving targets, as they constantly evolve amid the changing IT landscape. They need to be monitored continuously and the hybrid cloud environment correspondingly re-examined for its ability to meet new requirements. It is advisable to address this topic as soon as possible, as not doing so can leave an environment vulnerable to threats. Still, this can often be difficult to achieve with in-house IT resources.

Working together with a strategic partner familiar with the security requirements of hybrid cloud allows organisations to take advantage of this approach without having to constantly keep track of the latest developments. Contact Proact *here* to learn more about how we can support in developing a hybrid cloud security strategy for your organisation.



PROACT

#ThePowerOfData
#ThePowerOfTogether

info@proact.eu
www.proact.eu

About Proact

Proact is Europe's leading specialist in data and information management with focus on cloud services and data centre solutions. We help our customers to store, connect, protect, secure and drive value through their data whilst increasing agility, productivity and efficiency.

We've completed thousands of successful projects around the world, have more than 4,000 customers and currently manage hundreds of petabytes of information in the cloud. We employ over 1,000 people in 13 countries across Europe and North America.

Founded in 1994, our parent company, Proact IT Group AB (publ), was listed on Nasdaq Stockholm in 1999 (under the symbol PACT).