Reduce complexity in multicloud

With increased visibility, control and security

Design your cloud estate to secure your assets and provide 360-degree visibility

The adage “you can’t protect what you can’t see” has never been truer than when it comes to the cloud environment.

Moving to the cloud comes with many benefits including improving agility, while boosting productivity and cost efficiency. But there are also major challenges in terms of asset and data control, visibility and security.

Multicloud can significantly increase the size of your threat vista and requires the use of modern, readily-available protection mechanisms. The best and simplest design for your needs will depend on your multicloud platforms and vendors.

In a multicloud environment it is easy to lose sight of your data and where it is located. If you haven’t planned how processes and data will be organized in your clouds from the start, the dynamic way cloud works makes it extremely difficult to have full visibility on what is happening. Without this visibility, it is impossible to enforce consistent governance and compliance policies, to secure data and monitor for potential threats.

For example, look at the consequences a data breach could have on your organization. In addition to damaging reputation and customer loyalty, a data breach can have a huge impact on the bottom line. The Ponemon Institute estimates that the cost of an average data breach has risen 12% over the past five years, to an average of $3.92 million.[1]

Understanding cloud responsibility

Moving to the cloud doesn’t mean handing over responsibility or accountability. Cloud providers are constantly working to secure their clouds, but as a cloud tenant, you are responsible for the cloud estate they create.

77%

of enterprises have one application or part of their computing infrastructure in the cloud[2]

Four multicloud security best practices

- **Define your security policies and procedures before migrating to the cloud** as they will differ from the ones your organization already has.
- **Discover if your cloud provider has met industry security standards** such as SOC2, ISO 27001, ISO 20000-1 and the (ISC)² CCSP certifications.
- **Ensure you fully understand your cloud providers’ services, notably platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS).** In addition, ensure you understand the specifics and caveats of the services they are offering plus the responsibilities tied to each under joint security responsibility models.
- **Identify controls, such as infrastructure monitoring, with each cloud provider to monitor policies and procedures** to ensure your governance and compliancy needs are continually being met. Policies help you to outline the way users behave in the cloud, detecting risky behaviors, for example.

In addition to securing assets in the cloud, you need to know how to protect at scale, track and secure workloads across clouds. It is also important to deploy consistent security functionality and policies across different clouds. This isn’t an easy task when each cloud is built differently.

In multicloud, you are likely to be spinning up services in multiple data centers in different locations. This means complying with regulations from different host regions and managing varying contractual obligations with multiple providers. This creates a very complex picture, where unforeseen security vulnerabilities can cause expensive data leakage. Consequently, it is essential to improve your operational capabilities in the cloud and ensure your data and assets are safe and only visible to the right individuals.

Orange Business Services provides an a la carte menu of services that will help you with the migration and evolution of your business environment in the cloud. Your applications and infrastructure can be managed based on your requirements and adjusted to your team’s expectations. We achieve this through maturity assessments and careful cloud design, which extends to security and incident management.

1. Ponemon Institute 2019 Cost of a Data Breach Report 2. IDG Cloud Computing Study 2018

orange™ Business Services

Keeping the multicloud environment safe

As enterprises adopt more cloud services, monitoring data flows becomes a far bigger challenge.

Despite 76% of enterprises looking to cloud apps and platforms to speed up IT service delivery[3], many are still having difficulty with their cloud transformation. In the UK alone, 15% of enterprises say they are struggling to find the right partner to help them in their cloud implementation process.[4]

If an enterprise doesn't have extensive technical and legal skills, it is important to have a partner to help design a cloud environment, refine service, security and support capabilities, and help users understand the transformation required in moving to multicloud.

86%
of enterprises have a multicloud strategy.[5]

Get cloud-ready

Some enterprises are already in the second or third phase of their cloud adoption. When they first moved to cloud's pay-as-you go model, they often saw savings. But, if they don't have full visibility of their rapidly expanding cloud estate, they soon find multicloud is more expensive and complex to manage, and can expose them to more security vulnerabilities.

This is why it is vital to plan your cloud design and develop an optimized way of working in a multicloud environment. Our cloud consultants can help you develop a robust cloud design using a vendor-agnostic approach. They help you determine your objectives for moving to the cloud and carefully plan for them. For example, if you want to be more agile with shorter times to market, we design for this scenario. If you want to make substantial costs savings by moving to IT-as-a-service, we can help you reach this goal.

Don't always try to chase too many objectives at once. The biggest threat to enterprises migrating to the cloud is bad design. Data leak and data loss will become a big problem as you will be exposed to attack from anywhere in the world. Plan for cloud, monitor what happens, correct what is not in line, and then plan again. Because new services are being launched every week, control, visibility and security are an essential ongoing process.

orange™ Business Services

Five steps for control, visibility and protection over multicloud

1. **Have a cloud maturity assessment** on your cloud design to pinpoint any possible issues and ensure your primary objectives are clear.
2. **Run a security assessment** so that you fully understand and control the multicloud complexity you are dealing with.
3. **Understand the different strengths and weaknesses of your cloud providers** when it comes to control, visibility, security and optimization.
4. **Ensure your cloud design doesn't lock you in beyond what you are ready to accept** and that there is suitable security across all clouds.
5. **Prepare for the future and use appropriate security innovations services such as artificial intelligence (AI) and blockchain.** These innovations are key in extracting the most business value, while ensuring your data and assets are being protected for yourself, your users and all your customers.

Click here to find out more about how Orange Business Services can help you control and secure your data and assets, whilst ensuring maximum visibility.

3. IDG Cloud Computing study 2018.
4. Cloud Industry Forum – Cloud the Next Generation 2019
5. Forrester Research Multicloud report 2018.

Copyright © Orange Business Services 2019. All rights reserved. Orange Business Services is a trading name of the Orange Group and is a trademark of Orange Brand Services Limited. Product information, including specifications, is subject to change without prior notice.