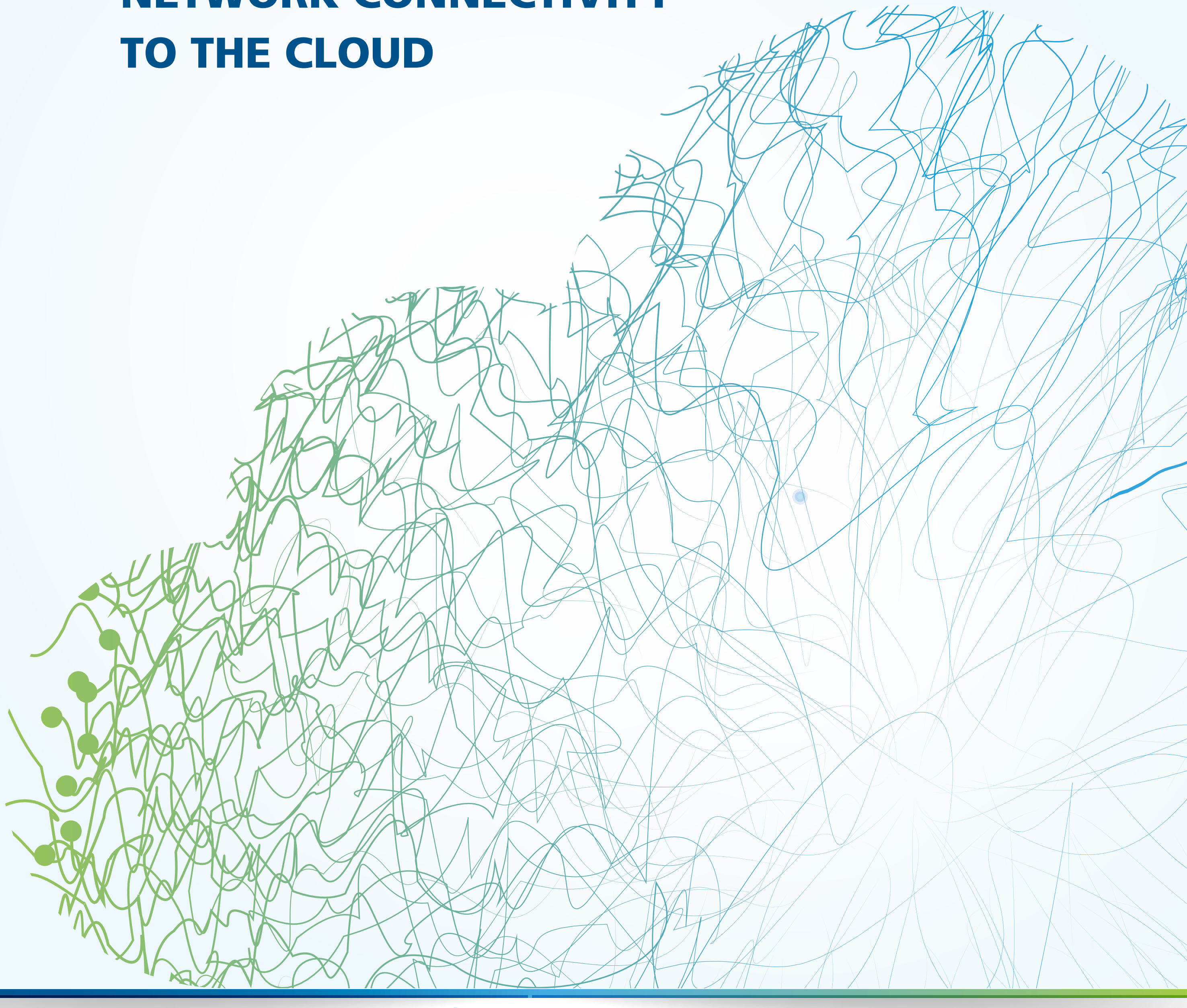
AN ALGOSEC WHITE PAPER

MIGRATE APPLICATION NETWORK CONNECTIVITY TO THE CLOUD

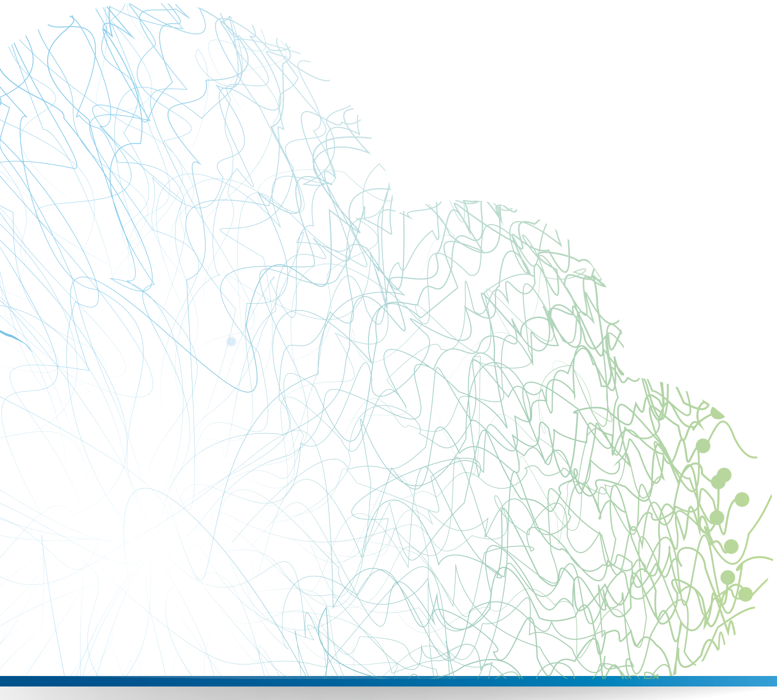


Responsiveness to the ever-growing demand coming from the business is redefining the IT processes and technologies. One way IT can improve responsiveness and business agility is by moving business applications to the cloud. In the cloud, businesses increase their agility while reducing costs. While migrating applications to the cloud, network security is often neglected. When this happens, applications are deployed in the cloud with inadequate security and compliance measures in place, or, conversely, the security team steps in and halts the migration process.

This puts the company at risk: inadequate security makes it easier for hackers to access the network and mount an attack against the company – exposing the company to financial losses and legal repercussions. Moreover, if the business is unable to respond to market demands in a timely fashion, there are clear financial implications.

In this paper, we will take a deep dive into the process enterprise organizations take when approaching a migration project. We will look at the challenges associated with migration projects and we'll discuss a systematic process that organizations should embrace when approaching these types of projects.

TABLE OF CONTENTS



ADVANTAGES AND SECURITY CHALLENGES OF THE CLOUD

There are multiple advantages for adopting the cloud and migrating applications to it, but there are also security concerns that need to be taken into consideration. Below are the top four advantages and the security challenge that comes with them:

Security and Data Protection

When adopting the public cloud, data itself is much more accessible, no matter where it is located. Users can access the data they need from any location and device. An additional benefit relates to disaster recovery processes that include out-of-the-box backup and restore functionality. In the cloud, there is a need to maintain additional servers in a remote location. These advantages do not come without a cost. Once the data is no longer kept on-premises, security must be tightened. The closed garden we had with data residing on servers protected by firewalls in our facilities is gone. Additional security controls must be employed. Special consideration should be taken with upholding regulatory requirements on the data itself. There are best practices to uphold, as well as financial penalties if organizations do not comply with them.

Business Agility

Spinning up a server in the cloud is a matter of minutes. Cloud computing is considered an enabler for digital transformation, as businesses work to be more agile and accommodating to their customer needs. All you need is a credit card. No hardware required to be purchased, shipped or connected to your data center. The easiness of spinning up a new cloud server makes shadow IT possible. This is also a security problem. It is hard to control the security aspect of each cloud server if you are unaware of it. Therefore, visibility and strong prefrail security measures such as identity management, and cloud firewalls that protect access from the Internet are needed. For each cloud server, you need to set a baseline of allowed connectivity and incorporate it into the creation process.

Financial benefits

The cloud offers zero maintenance cost and zero capital cost. Additional financial gains should be taken into consideration such as the reduction in IT support cost, the flexibility that comes with the cloud server usage so that you pay only for what you consume. This means you don't have to purchase expensive hardware that you would only need during peak times. Of course, there are also hidden costs when migrating to the cloud. Usage needs to be monitored and optimized and your cloud assets need to be monitored and maintained. Additional security measures need to be put in place. This includes purchasing additional software as well as additional proficient personal that need to be hired to making the cloud secure.

Faster time to market

The cloud, coupled with DevOps practices and tools, delivers a flexible framework that enables companies to deliver innovations faster to market. However, there are lingering questions about its impact on security. With multiple functional teams collaborating on development, and so many moving parts in the process, security is often not incorporated into the release process. Rather it's tacked on at the end.

And this is where you need a security policy automation that supports the DevOps methodology. This solution needs to be able to automatically copy the firewall rules – and then make the necessary modifications to map rules to the new objects, when the rules are applied to each new environment in the DevOps lifecycle. With the right automation solution, security can be baked into the release process.

THE SHARED RESPONSIBILITY MODEL

Public cloud security is the responsibility of both the cloud vendor and cloud customers. This joint ownership of security is often called the shared responsibility model.

On one side you have security of the cloud infrastructure itself.

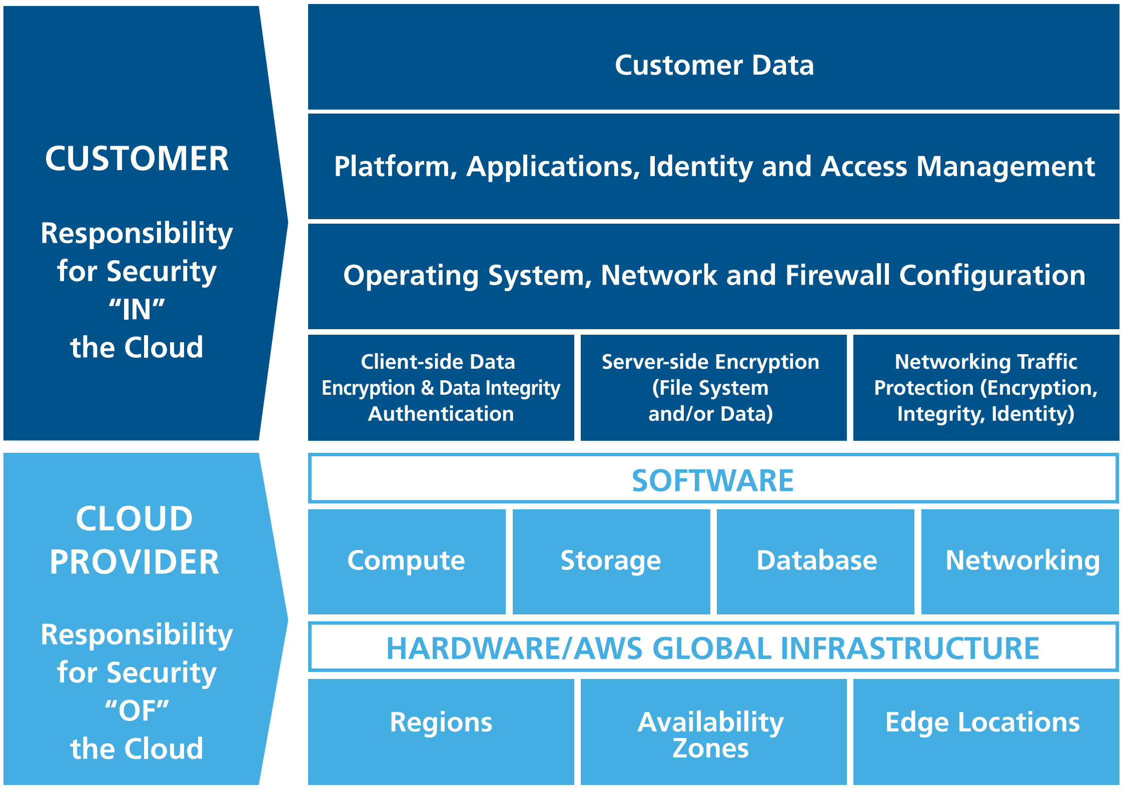
Security *OF* the Cloud

The cloud vendor is responsible for securing the infrastructure that runs all the services offered in the cloud. This includes both software-related services such as compute, storage, database, and networking as well as hardware services. The cloud vendor is also responsible for securing the physical facilities themselves.

On the other side, you have security within the cloud accounts.

Security *IN* the Cloud

Cloud customers are responsible for the security of the services they consume. For example, when using Amazon Elastic Compute Cloud (Amazon EC2) the customer needs to perform all the necessary security configuration and management tasks. Any software or utility that the customer installs should be followed by configuring all relevant security controls, including security groups, third-party firewalls and other needed security configurations. Cloud customers are responsible for managing and securing the data that resides in the consumed cloud service.



CUSTOMER

Responsibility for Security "IN" the Cloud

Customer Data

Platform, Applications, Identity and Access Management

Operating System, Network and Firewall Configuration

Client-side Data Encryption & Data Integrity Authentication	Server-side Encryption (File System and/or Data)	Networking Traffic Protection (Encryption, Integrity, Identity)

CLOUD PROVIDER

Responsibility for Security "OF" the Cloud

SOFTWARE

Compute	Storage	Database	Networking

HARDWARE/AWS GLOBAL INFRASTRUCTURE

Regions	Availability Zones	Edge Locations

Figure 1: Shared responsibility model

CLOUD NETWORK SECURITY CONTROLS

Data center network security is already quite complex. Customers are utilizing multiple vendors to manage their network security, including SDNs, such as Cisco ACI and VMWare NSX. With the cloud network security controls in the mix, the complexity is immense.

Cloud network security consists of multi-layered security controls. You have the cloud vendor infrastructure controls spanning across asset types, such as instances, databases, storage, and accounts to configuration types, such as deployment location, security groups, and more. You also have cloud providers' security products, such as Azure Firewall and AWS WAF. To top all of that, third-party vendors have not left the cloud network security controls ring and are providing dedicated firewalls for the cloud, such as CloudGuard by Check Point, V-Series by Palo Alto Networks and more.

When migrating an application to the cloud it is important to determine how are you going to guard your cloud assets. What will be the mix of security controls that you are going to utilize to secure your data.

VISIBILITY TO WHAT YOU HAVE IS KEY FOR CLOUD MIGRATION

Gain Visibility to Which Application Your Organization Has

Obtaining an inventory of applications is the foundation of your security and essential for your cloud migration. The process of discovering all the applications used by your business is not a trivial task. Most businesses have two types of applications – enterprise and departmental. Enterprise applications, the more complex applications in your data center, usually serve many business units and can span multiple geographies and even company subsidiaries. In most cases, the IT team is well-aware of them. While the documentation of these applications with their connectivity requirements may not be perfect, that is a good starting point for the migration process. Note that there may still be a need to update the documentation. Many departments or business units purchase their department applications such as Business Intelligence solutions or project management tools. Some of these applications may be SaaS while others are installed on corporate servers. For these types of applications, it is likely that documentation never existed. Fortunately, in most cases, their architecture isn't complex. It should be relatively easy to obtain the necessary connectivity information needed to migrate them to the cloud. However, the key here is to know that these applications exist. There are two ways to generate a list of applications. The first requires using consultants to conduct thorough interviews with the various stakeholders in each department and each geography. A second, more cost-effective and efficient way, is by using visibility and automation solutions such as AlgoSec AppViz and AppChange. Tools like AlgoSec AppViz help discover, identify, and map business applications on your network. Once the list of applications – the foundation – is in place, you can move onto the next stage in the process of closing the security gap as you migrate to the cloud: understanding each application's attributes, such as the number of servers, associated business processes and network connectivity requirements. These attributes help determine the complexity involved in migrating applications.

Gain Visibility to Your Current Network and Its Security Elements

Several attributes can affect the complexity of migrating an application to the cloud, including the application's network connectivity requirements and the firewall r ules t hat a llow/ deny that connectivity. Mapping network connectivity provides a deeper understanding of network traffic complexity which, in turn, provides insight into the flows you will need to migrate and maintain with the application in the cloud (see Figure 2). Additionally, this information will tell you how many applications are dependent on a specific server. The more applications that utilize a server, the harder it is to migrate an application that depends on that server. It may be necessary to migrate the server itself or to migrate multiple applications at the same time.

Mapping the firewall rules provides insight into the security measures you will need to put in place once the application has been migrated to the cloud. As a rule of thumb, the more firewall rules are required, the greater the complexity. This mapping allows you to identify and decommission firewall rules that are no longer necessary post-migration. So how do you generate documentation of application connectivity? The obvious choice is to employ a solution that automatically maps the various network traffic flows, servers and firewall rules for each application. If you do not have access to such an automation solution, manually documenting, however tedious, will provide the necessary information.

WHICH APPLICATIONS SHOULD I MOVE FIRST?

Applications That Store Data About Personal Information

When an application holds sensitive data like personal information it is worth thinking twice before moving it to the cloud. In most instances, regarding personal information, many data privacy laws mandate where data is stored, when is the information collected, processed, or communicated. Over 80 countries and territories have adopted comprehensive data protection laws. Most of Europe has already adopted comprehensive data protection laws such as GDPR. Many Latin American, Asian, and African countries have done so as well. Many US states also have data protection regulations such as the California Consumer Privacy Act and the New York SHIELD Act. It is worth checking what is allowed from a legal perspective before moving such an application to a cloud as well as the geographical location of the cloud that is being used.

Highly-regulated Applications

An additional sign to look out for is if the application is subject to regulatory requirements such as HIPPA or requires PCI DSS compliance. If the answer is yes, then there is a need to understand the security compliance status of that application and if moving it to the cloud will violate it. For example, HIPPA requires accountability practices on all Local Area Networks, Wide Area Networks, and for users accessing the network remotely through a Virtual Private Network (VPN). Or if you need to be PCI compliance you will need to have a firewall at each internet connection and between any DMZ and the internal network zone. Applications under this regulation and others are not the best candidates to be moved to say the least.

Application Already Exposed to the Internet

On the other hand, if there are already elements of the application that are exposed to the Internet, like the web server in Figure 2 below, it is a good sign that maybe some of it if not all can be moved to the cloud to get the elasticity and cost savings needed. Most probably, for these applications, you have already implemented strong security inside the application server, and it is backed with strong security limitations in front of and behind the web-facing interface. Adopting these strong limitations when moving the workload to the cloud will ensure the security of the server and also the internal network that is behind it.

Network Segmentation as a Telling Sign

Finally, if you manage your network segmentation correctly, the servers and applications that reside in the less isolated zones are the best candidates to move to the more open cloud. For example, applications and servers that are in the zone that has only one firewall that acts as a barrier between the zone and the Internet are good candidates to be moved. Whereas, those zones that are highly protected, like server group 1 in Figure 2, and resides behind several firewalls should stay in your data center.

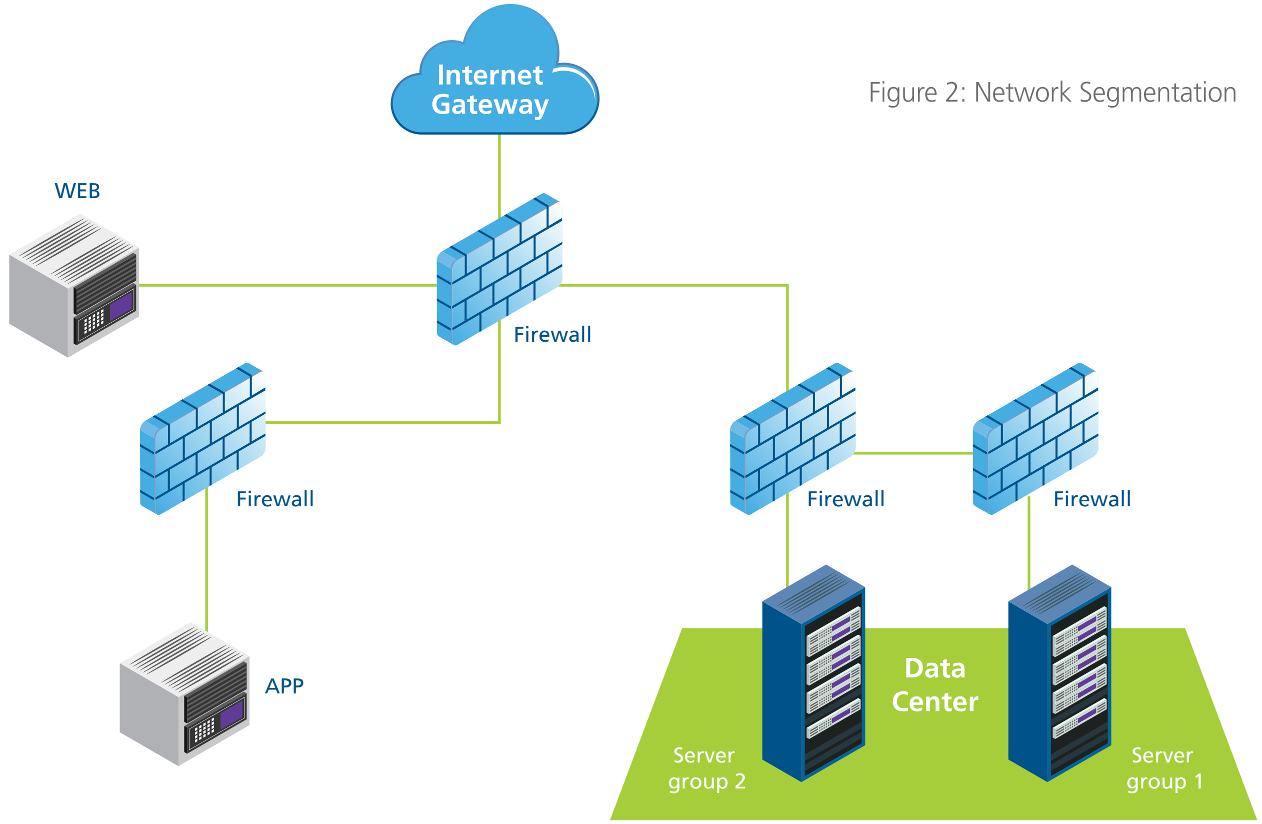


Figure 2: Network Segmentation

MIGRATION IS ONLY THE BEGINNING

Whether you move all your applications to the cloud or just a few of them, and whether you use one or multiple cloud vendors, you now need to manage and maintain the security and compliance in the cloud just as you did in your on-premise network over which you have complete control. Establishing a route from a server in the cloud to a server on the on-premise network requires an intimate understanding of both the cloud security controls and the on-premise security devices. Where there are separate cloud and on-premise network security teams, as is the norm in many businesses, collaboration between the teams is needed which, of course, adds its own complexity. Once applications are deployed in the cloud, you will likely want to be able to move between cloud providers 'at the speed of the cloud' to avoid vendor lock-in and to minimize costs. While you might be led to believe that this is a simple requirement, in reality, each cloud provider has its own, unique network security controls with which you need to familiarize yourself. There are several ways to manage security across the hybrid cloud environment.

1. You can manage the environment manually, which is slow, time-consuming, and error-prone.
2. You can use the cloud provider's native controls to manage the cloud network security in addition to the existing tools and methodology you currently use for your on-premise environment. However, bear in mind that cloud security controls do not provide a holistic view of security across your entire estate and their limited capabilities may not sufficiently support your business's security posture.
3. Alternatively, there are third party automated network security policy management solutions that span the entire hybrid environment which can assist in managing the entire network security

MIGRATE WITH ALGOSEC

The AlgoSec Security Management Suite (ASMS) makes it easy to support your cloud migration journey. Ensuring that it does not block critical business services and meet compliance requirements.

AlgoSec's powerful AutoDiscovery capabilities help you understand the network flows in your organization. You can automatically connect the recognized traffic flows to the business applications that use them. AlgoSec seamlessly manages the network security policy across your entire hybrid network estate. AlgoSec proactively checks every proposed firewall rule change request against your network security strategy to ensure that the change doesn't introduce risk or violate compliance requirements.

ABOUT ALGOSEC

AlgoSec enables the world's largest organizations to align business and security strategies and manage their network security based on what matters most - the applications that power their businesses. Through a single pane of glass, the AlgoSec Security Management Solution provides holistic, business-level visibility across the entire network security infrastructure, including business applications and their connectivity flows — in the cloud and across SDN and on-premise networks. With AlgoSec users can auto-discover and migrate application connectivity, proactively analyze risk from the business perspective, tie cyber-attacks to business processes and intelligently automate time-consuming security changes — all with zero-touch, and seamlessly orchestrated across any heterogeneous environment. Over 1,800 leading organizations, including 20 of the Fortune 50, have relied on AlgoSec to drive business agility, security and compliance. AlgoSec has provided the industry's only moneyback guarantee since 2005.

algosec | BUSINESS-DRIVEN SECURITY MANAGEMENT

AlgoSec.com