A CISO'S GUIDE TO HYBRID CLOUD SECURITY

Achieving Continuous Security and Compliance Across Azure, AWS, and NSX

White Paper Contents

Today, integrating the public cloud in some capacity is becoming an integral component for the strategic future of most businesses. The benefits are near irresistible. From flexibility and velocity, to business agility, clouds are essential in helping businesses meet their objectives. A well-respected consultant at Eli Lilly and Company once **remarked** that it used to take them over seven weeks to deploy a server internally. But with the addition of cloud computing, a new server can be up and running in three minutes or less

So the question is no longer *if* an organization will adopt the public cloud, but rather *how many* of these cloud platforms they will they leverage. At the pace that shadow IT is taking it upon themselves to embrace public clouds for the agility it provides, security professionals often end up in the position of owning security and compliance for both their existing and new infrastructure, whether that infrastructure is VMware NSX, Microsoft Azure, AWS, or other cloud platforms.

It is within this context that we will focus on. This is a guide for CISOs who are struggling with security and compliance for their growing hybrid cloud environments, facing challenges in three key areas:

- Visibility
- Compliance
- Consistent policy across environments

Yet major challenges exist when deploying public and hybrid cloud environments. From managing multiple or diverse security technologies, to ensuring all technologies are configured to work together, navigating the nuances between the various cloud platforms can tax most IT departments and present headaches to security teams. Specifically, securing data and applications that cross hybrid clouds represents a major security concern.

Rethinking Security based on the Evolution of the Application

CISOs striving in a hybrid cloud environment to improve visibility, compliance, and consistent policy across platforms should start by understanding the nuances of complex business applications. Today, when we think about applications, we need to consider how they have changed over time from simple, autonomous entities to complex business applications, workflows, operations, and policies that are often interwoven with other applications throughout an entire enterprise.

Consider, for example, a complex application like the Society for Worldwide Interbank Financial Telecommunication (SWIFT). A message format by SWIFT was adopted as the global standard for interbank financial transfers. Today, this associated software and messaging network drives the majority of international banking transfers, and can exceed **five billion** financial messages a year.

As a high value target, attacks on the SWIFT network have since been reported in Vietnam, Ecuador, and Ukraine, though the majority of banks and countries affected by the dozens of breaches being investigated have not been made public.

One of the main reasons SWIFT was such an enticing target was the intricacies between all the complex business applications that made-up a successful SWIFT business transaction, as well as often ineffective means of securing the complete SWIFT process. In response, SWIFT released a Customer Security Programme that provided guidance to financial institutions for improving security protections around the Swift Alliance Software – or any custom applications that interact with the SWIFT network.

But securing a SWIFT application stack remained dubious since many components of SWIFT applications are typically run by legacy physical systems and application stacks. This means that although the Customer Security Programme was a step in the right direction, many financial organizations were still unable to support newer security software or receive security updates to legacy systems. A common practice in previously defending SWIFT was to use numerous single instance firewalls and other segmentation technologies. The problem with this approach is there is no unified view across platforms, or single place to manage policies and controls distributed across all of the platforms.

At the center of this and other successful attacks is the fact that modern applications aren't simple any more. Components of most applications, today, can be distributed across containers, platforms and clouds. The evolution of the application, from simple software to a complex set of business services and solutions, is now spread across a wide-spectrum of internal and external servers. This evolution causes some of the most significant cybersecurity challenges for many organizations. CISOs who dive deeply into these differences between traditional and modern applications discover three main challenges: visibility, compliance and security:

HYBRID VS MULTI CLOUDS

Many users often interchange the terms multi-clouds and hybrid clouds. The hybrid cloud pertains to a network topology that consists of an internal, on-premise, cloud and the addition of one, or more, public clouds. The multi- cloud, on the other hand, is simply a series of public clouds. The challenge with these platforms is achieving visibility and compliance, as well as the consistent policies, IT departments need across the various environments.

Visibility

The complexity of modern applications hinders a CISO's – and an IT department's – ability to understand the communication dependencies and relationships that security professionals face in identifying what complex applications are running in their environments. This lack of visibility also leads to challenges with identifying dependencies that security administrators need in order to create more granular, intent-based policies that keep applications secure.

Compliance & Security

According to Marc Woolward, CTO at vArmour, complex business apps are more decentralized and stretched between clouds. “The stretching of complex business applications across clouds and platforms expands the attack surface. This also makes compliance more reactive and hinders a company’s ability to continuously monitor and take a proactive posture in upholding compliance.”

There are a few different approaches IT security leaders can make to try and create policies and secure hybrid cloud applications. Some common methods are using agent-based technologies, which can be cumbersome to deploy. Another common security approach is implementing firewall policy management solutions. The common challenge with these approaches is that they often centralize the administration, but still require IT teams to manually create all of the policies.

When working against aggressive provisioning timelines for new applications IT security is often an afterthought. As a consequence, the security team is commonly engaged late in the provisioning stage, so the security team often falls back to a legacy approach of just dropping a legacy firewall in place to meet requirements. Unfortunately, these legacy platforms often lack the granularity offered by modern cloud-native security controls, such as microsegmentation.

This approach may also look okay on paper, but in reality, it is a risky approach since there is no defense in depth, past the firewall. Once a cyber-attacker infiltrates or bypasses the firewall, there is nothing to prevent horizontal movement, lateral visibility is unavailable, and no protection for any assets in connected clouds exist. In order to mitigate this, CISOs and security teams need to leverage embedded controls for achieving east to west security behind the cloud perimeters established by firewalls. In practice, doing this effectively requires a subject matter expert (SME) per public cloud platform since there are different security features per platform and varying inconsistencies in terms of capabilities between platforms.

Adding to the Challenges of Decentralized Applications

Moving to multiple public clouds brings additional challenges, from a lack of cloud – or platform – specific expertise in security controls, to the need to understand the difference between managing data effectively between, and within each cloud. As complex business applications become more common across hybrid clouds, control issues between the various cloud platforms arise, creating challenges with regards to data migrations to the cloud.

Although most cybersecurity programs these days perform some sort of scanning, sandboxing or traffic examination to look for anomalies that might indicate the presence of malware, this is not enough to fully protect a modern, hybrid cloud environment. These technologies do not fulfill the fundamental security 101 approach of segmenting workloads from one another in order to minimize exposure and attack surface.

Expertise, Resources and Security

The speed and ease of implementing public clouds makes it all too easy for application owners to provision new applications without properly involving security teams, or properly deploying security policies themselves. Organizations must have SME's in order to properly protect information and resources housed in these newly provisioned apps. The need for security experts and solution architects to understand the differences between the various cloud platforms is also essential in order to drive improved data protection.

For example, security constructs like AWS' Application Security Groups differ drastically in usage from Microsoft's Network Security Groups. CISOs also need, yet often lack, the resources and expertise within their teams necessary to decipher the differences between various cloud platforms. For example, Azure has a prioritization per rule order while AWS does not. There are also vast differences in systems limits, such as the number of total rules and how they are applied to the objects or groups they are securing per platform.

Understanding and acting upon the differences of these features can help drive more effective security across all cloud environments. How? Here's an example that I'm sure you can relate with. Like many people, you probably have that drawer at home full of remote controls, each one controlling a different Audio/Video device. If you have upgraded to a universal remote, you know the beauty and simplicity of hitting a single button to watch TV. All at once, your TV turns on, your stereo turns on, and the stereo input is automatically changed to the correct setting. No fumbling with different remotes and no trying to remember what button does what.

However, in reality, a centralized controller is a good first step but not enough either. CISOs also need to incorporate a new approach that centralizes the clouds but that also leverages specific machine learning and heuristics algorithms to determine the workloads that make up various complex business applications in order to achieve true cloud security, compliance, and complex application defense before the worst happens, a breach.

Cloud Cybersecurity Challenges

There's no question about the business value of the cloud. The question thus becomes how to adapt security to work within hybrid clouds. Gemalto's Breach Level **Index** shows that on average, 291 records were stolen or exposed every single second in the first half of 2018. Gemalto's study also states that in the first half of 2018, those breaches led to a whopping 4.5 billion data records being compromised worldwide. Although the total number of breaches were down year-over-year, the number of records compromised rose by 133 percent, as did the severity of all reported incidents.

"Malicious outsiders caused the largest percentage of data breaches (56 percent), a slight decrease of almost seven percent over the second half of 2017 and accounted for over 80 percent of all stolen, compromised or lost records," the Gemalto's Breach Level **Index states**.

Compliance is also a big problem, especially within cloud environments. Whether it is GDPR, PCI-DSS, HIPAA, SWIFT or any number of regulatory requirements imposed in tightly controlled sectors, meeting those requirements is always going to be challenging. One of the main reasons for the difficulty regarding compliance is the fact that hybrid cloud platforms introduce more complexity into compliance structures for organizations. From the increase in the number of vendors to the different naming conventions and APIs that hybrid clouds require, the need to simplify this platform is essential to driving proactive and continuous compliance versus reactive compliance.

SIMPLIFYING COMPLIANCE

In striving to achieve PCI-DSS compliance, all the security administrator needs to do with vArmour is select sets of the PCI-DSS servers that are already auto-discovered by the solution, and then simply apply the PCI-DSS Compliance template to generate candidate policies.

Organizations need to bolster security by delivering consistent, automated protections across all public and private clouds, as well as hybrid environments. This represents the best approach towards providing the capabilities to adopt Software as a Service applications and avoid business disruption while quickly launching cloud-enabled services and capabilities. This approach also should include centralizing and simplifying hybrid cloud administration and abstracting the nuances and differences per public cloud platform. This approach not only drives better defense but also reduces the need for a large team of subject matter experts per cloud.

Accelerate Cloud Security with Workload Isolation

By leveraging machine learning models to define every process, application and workflow needed to conduct business, CISOs can achieve a level of workload isolation that helps identify critical programs along with all interactions. This is an essential element in securing hybrid clouds without needing to deploy agents and regardless of the hardware infrastructure used to secure each cloud environment. It's also a simpler way to manage and secure data that stretches across platforms.

Workload isolation is also a different way to approach security that defines everything that is allowed within a network, versus having to spend time searching for behaviors that might indicate a threat. "At the very least, critical functions can be identified and all interactions with them are constrained and monitored," said Marc Woolward, CTO.

Simplified Defense and Management, with Compliance

Workload isolation can work in any environment, whether in massive data centers or sprawling public clouds. But only a solution like the vArmour Application Controller leverages machine learning and sophisticated algorithms to simplify the provisioning of robust security capabilities and full workload isolation. In addition to increasing security, it simultaneously simplifies the entire cybersecurity process by dynamically providing the visibility that identifies workload types, application clusters, and dependencies so that security administrators can easily understand application relationships and create granular, intent-based policies, without conducting any manual operations.

This single-console capability within vArmour automatically centralizes and simplifies the operation of hybrid clouds while keeping an enterprise both secure and compliant. Also, since vArmour can automatically compute the security policies needed for compliance, the solution removes the manual process of mapping all the workloads relative to a compliance requirement. The solution also removes the manual process of creating policies for each individual workload.

Additionally, features like vArmour's Conform technology addresses anxiety among security teams struggling with their organization's rapid adoption of hybrid cloud platforms, whether the expansion be to Microsoft Azure, AWS, VMware NSX, or others. Conform bridges security and compliance policy requirements to public and private cloud. Without Conform, security and IT teams are left to the overwhelming task of reconciling policy rules, platform capabilities – and other nuances that differ – to their disparate cloud environments, each with its own unique security controls and nuances.

Finally, the vArmour suite also enables seamless deployment of consistent application communication policies and fully validates them, which further bolsters hybrid cloud security by enforcing those critical policies across hybrid cloud environments. This eliminates the complexity of managing hybrid or incompatible security technologies, and ensures that the entire environment, regardless of its configuration, is working properly, fully compliant with all applicable standards, and always working at peak effciency.