3 Strategies for Securing Multicloud Networks

Published 1 November 2021 - ID G00753279 - 15 min read

By Analyst(s): Aaron McQuaid

Initiatives: Infrastructure Security

The migration to multicloud environments forces security and risk management leaders to rethink their network security architecture. They must understand what mix of cloud-native controls, virtual network firewalls and physical firewalls at colocation hubs is optimal to secure this new architecture.

Overview

Key Findings

- While network security principles remain largely the same, the underlying architecture and operations of hybrid environments are often vastly different (for example, the concept of Layer 2 switching does not apply to public cloud networking). Security teams sometimes struggle to have principles applied uniformly across the many options available to their multicloud computing environments.

- Organizations adopting a public cloud expect to benefit from increased agility, platform modernization and greater operational efficiency, but securing a public cloud with a poorly designed security architecture negates these benefits. Adding third-party controls can introduce operational friction and negate some of the benefits inherent to public cloud adoption.

- Cloud-native security controls are increasing their efficacy over time, but they have not yet reached parity with traditional appliance-based security controls.

- In a multicloud scenario, organizations often choose third-party security controls to unify security policy and management across on-premises and cloud instances. This unified approach decreases management complexity at the cost of increased operational complexity.
Recommendations

Security and risk management leaders responsible for infrastructure security should choose from the following three network security architecture approaches to public cloud design:

- Adopt the cloud-native security control design as your starting point when cloud-native security controls satisfy your organization’s minimum security policy and the increased granularity offered by third-party virtual appliances is not required. Also adopt this design if minimizing operational friction for continuous integration/continuous deployment (CI/CD) pipelines is a major requirement.

- Adopt the third-party virtual appliance design if your organization’s minimum security policy for north/south traffic cannot be met with cloud-native controls and your organization is geographically dispersed with moderate bandwidth and high-availability requirements.

- Adopt the colocation hub design if your organization’s minimum security policy for north/south traffic cannot be met with cloud-native controls and you require very high bandwidth and subsecond high availability. We recommend adopting this design selectively for regions where your user density is very high.

Introduction

Most organizations have already embraced public cloud computing. Others are in the process of migrating to public cloud services. Infrastructure as a service (IaaS) is currently a $79 billion market and is estimated to be the fastest-growing public cloud market, with a forecast compound annual growth rate of 29% for the period 2020 through 2025 (see Forecast Analysis: Public Cloud Services, Worldwide, 1Q21 Update).

Many organizations initially try to “forklift” their on-premises controls to the cloud, without much success. Conversely, cloud operations teams often enable cloud-native security controls without the oversight of the security team, which leads to poor orchestration and inconsistent security. Further complicating these problems is the fact that many organizations repeat their mistakes with multiple cloud providers, due to the trend for multicloud adoption. Gartner’s 2020 Cloud End-User Buying Behavior Survey found that adoption of multicloud infrastructure is prevalent among 76% of respondents (see Quick Answer: Who Is Adopting Multicloud Infrastructure?). As a result, security and risk management leaders need to establish or reset their network security strategy. This research highlights three design models for network security for the growing multicloud world.
Security and risk management leaders must adapt to how fast their organizations choose to embrace cloud computing. They may be forced to compromise with development teams to ensure operational efficiency. Most organizations start with cloud-native security controls as development teams and line-of-business IT organizations typically adopt cloud computing with minimal involvement of the security team. But as organizations mature their public cloud use, they realize that cloud-native security may not meet all the requirements of a security architecture. This leads many security teams to look at third-party security controls or, in some cases, deploy physical security controls at a colocation hub for the most direct control over the network security stack. Security and risk management leaders need to integrate standardized security architectures into the software development life cycle, so that security controls can be deployed at the scale and speed required by development teams. They also need to ensure that operational friction is minimized, so that security compliance is not viewed as an impediment to development progress.

The three multicloud security designs that Gartner recommends choosing from are (see also Figure 1):

1. **Cloud-native controls with no third-party security solution**: Cloud-native controls with a common automation plane for CI/CD pipelines. Cloud-native controls are used to secure both east/west and north/south traffic. This architecture is the most “cloud-native” as it uses native security controls with a common automation tool like Terraform or Jenkins.

2. **Third-party virtual appliance**: A virtual appliance is used to secure north/south traffic flows, while cloud-native controls secure east/west traffic. This architecture integrates a third-party perimeter gateway at the edge (firewall, web application firewall [WAF] or VPN) of each public cloud. It provides a common management framework for cloud edge security and greater security efficacy and granularity over cloud-native controls. For increased security, an identity-based microsegmentation platform can be deployed for east/west traffic (typically, an agent-based approach that performs segmentation based on server tags is used for public cloud IaaS deployments). See further Three Styles of Identity-Based Segmentation.
3. **Physical security stack at a colocation hub**: A physical security stack at a cloud-adjacent colocation hub is used to secure north/south traffic, while cloud-native controls secure east/west traffic. This architecture serves as a bridge between legacy deployments and newer cloud-centric deployments. Teams from more traditional industries may prefer the idea of having a physical appliance stack or a network function virtualization (NFV) stack to act as a “digital edge” for public cloud access. This physical security appliance can support a multicloud deployment as most colocation hubs are geographically adjacent to the three main public cloud service providers.

Figure 1: Three Network Security Designs for Cloud

In addition to network-focused security controls, security and risk management leaders must consider implementing a cloud security posture management (CSPM) platform to ensure that the baseline cloud security configuration is correct for all cloud objects (see Market Guide for Cloud Workload Protection Platforms).
What Types of Security Controls Should We Use to Protect Public Cloud Workloads?

Some workloads arising from established application types, such as CRM, ERP, payroll and collaboration applications, are commonly offered via established SaaS platforms. SaaS deployments often have a lower total cost of ownership and are simpler to secure than IaaS deployments, so we recommend investigating SaaS options where possible.

When considering IaaS, organizations that were not “born in the cloud” often struggle with the question of whether to use cloud-native security controls or stick with traditional on-premises security controls.

When an organization begins to move workloads into a public cloud, a “crawl, walk, run” approach is recommended. Most organizations start with a private WAN link to the public cloud with cloud-hosted workloads being front-ended by the existing on-premises data center security stack. The intermediate phase involves hosting a subsection of workloads in the public cloud with direct internet access. This raises the question of how to secure these workloads, now that they are no longer being protected by the data center security stack. This is a critical phase of the journey toward cloud adoption because, if it does not go well, it can impede the speed of cloud adoption and endanger the process of becoming a “cloud-first” enterprise. This often gives rise to a technical and philosophical debate between internal cloud and security engineering/architecture teams.

Most organizations start securing cloud workloads in a silo. Cloud operations teams enable native controls because security teams are not ready to offer better solutions. Then security teams try to forklift their existing on-premises security controls, cutting corners but ignoring key paradigm differences. Most security teams have a gut instinct that prompts them to implement known enterprise firewall/WAF solutions in the cloud. Only later, as both teams realize that a long-term standard is needed, will they agree to adopt a common framework, which may consist of only cloud-native controls or a combination of cloud-native and third-party controls. If a security team can standardize on a mutually agreed approach before moving to the cloud, a large amount of engineering rework can be avoided.

Analysis
Cloud-Native Controls With No Third-Party Security Solution

Public cloud service providers provide many native security offerings, including identity-based segmentation, intrusion detection system, network firewall, WAF, API gateway, distributed denial of service (DDoS) mitigation, and identity and access management offerings. In this design approach, no third-party security controls are used. This approach provides the greatest scalability because it is the easiest way to completely automate production infrastructure as code. Most public cloud providers focus on firewalls, WAFs and VPN (LAN to LAN) gateways. More advanced controls, such as intrusion prevention systems, network detection and response, and sandboxing, may not be available.

Figure 2 illustrates cloud-native controls with no third-party security solution.

**Figure 2: Cloud-Native Controls With No Third-Party Security Solution**

Cloud-native controls have major strengths, including:

- NSG = network security group; VPC = virtual private cloud; WAF = web application firewall
The main weaknesses of cloud-native controls are:

- The lack of policy granularity/efficacy (usually limited to Layer 3 of the OSI model and less mature policy management software).
- The lack of a unified management console across cloud service providers.
- Disparate security control options across multiple cloud service providers.
- The security team's likely deep level of knowledge about incumbent third-party controls.

Some cloud-native controls may not include all the features of, or have the same granularity level as, third-party security products, but do they apply the right controls for the risk and value of the assets being protected in the cloud? There is no universal answer to this question. We recommend conducting a proof of concept to compare cloud-native and third-party controls in order to find the right answer for your organization.
Since the majority of large enterprises want to avoid vendor lock-in, multicloud is a common strategy. In a multicloud deployment, one of the major issues for security and risk management teams is the requirement to master two or three sets of cloud management and configuration platforms. The duplication of effort involved in this undertaking is compounded by the fact that cloud-native security control offerings are not uniform across all major cloud service providers. Thus organizations need to ensure that their cloud security teams are fully trained on all relevant platforms and that they apply consistent security policy across all platforms while utilizing different controls. We strongly recommend using a CSPM product in such circumstances to automate security policy and ensure it is correctly implemented.

The issue of existing expertise in third-party controls is only half the equation. Deploying workloads at scale in a public cloud with either native or third-party controls requires deep programming knowledge. Most cloud professionals have programming skills (and focus on application development, not security), but most traditional security or network engineers do not. To deploy third-party security controls in a public cloud, one needs staff with expertise in the cloud platform, the third-party controls and programming. People with all three skills are hard to find, and it is difficult to train internal staff to that level. Security and risk management leaders must account for these unique skill sets when deciding to deploy cloud-based workloads.

Third-Party Virtual Appliance

In situations where cloud-native controls are unsuited to the risk and value associated with assets that need protecting in the cloud, it is necessary to deploy third-party controls. Typically, these third-party controls are virtualized versions of an on-premises security appliance that are deployed as virtual machines on top of a public cloud provider's IaaS platform. These third-party virtual appliances are normally deployed as edge devices to inspect north/south traffic that moves between the public cloud and the public internet. A common design approach is to locate the virtual appliances inside transit or edge virtual private clouds (VPCs). A transit VPC acts as a demilitarized zone and front ends the various application VPCs. East/west traffic between application VPCs and intra-VPC traffic is segmented with cloud-native network security groups (NSGs) for scalability reasons. If one attempts to segment east/west traffic with virtual appliances, one can quickly see a deployment increase to hundreds or even thousands of virtual appliances. As an alternative, one may retain a virtual appliance in the transit VPC for controlling north-south traffic, but deploy cloud-native and/or third-party identity-based segmentation tools (agent-based microsegmentation platforms) to secure east-west traffic in public and hybrid cloud scenarios.
Figure 3 shows the third-party virtual appliance design.

**Figure 3: Third-Party Virtual Appliance Design**

The main strengths of the virtual appliance design are:

- Deployment of security controls developed by security vendors that focus on advanced threat intelligence and security features to deliver more security efficacy and policy granularity.

- A common management platform for security controls across multiple public cloud platforms and on-premises environments to enable operational simplicity by, for example, enforcing a separation of duties between cloud administrators, developers and security teams.

- A common set of security capabilities across multiple public cloud platforms with a common configuration and policy language.
Weaknesses of the virtual appliance design include:

- High-availability limitations.
- Bandwidth limitations.
- Deployment complexity.
- Added cost.

High availability is less robust and much more complex for virtual appliances than for traditional network security appliances. Due to the limitations of public cloud IaaS platforms (especially the lack of traditional Layer 2 connectivity), subsecond failover between redundant appliances cannot be achieved. It typically takes 15 to 60 seconds for one virtual appliance to failover to the standby virtual appliance.

Bandwidth is also limited on a virtual appliance, due to the limitations of virtual machines. Physical appliances can typically scale to 40 Gbps or more when clustered, whereas virtual appliances are usually limited to the 1-to-5-Gbps range, due to vendor and/or cloud provider limitations.

Deployment complexity is a major concern for the virtual appliance model. Third-party images need to be integrated into the cloud provider’s CI/CD pipeline process, and this is considerably harder than using a cloud-native-only design. Two instances of the virtual appliance must be deployed for high availability, and device configurations must be pushed programmatically as part of the CI/CD pipeline. A CI/CD pipeline that includes multiple third-party virtual appliances will be more complex than one that includes only cloud-native controls. Increased routing complexity is also introduced as you must program the cloud to route traffic to and from the virtual appliance while double checking that there is no route around the virtual appliance. The skill set required for this is significant and requires advanced knowledge of the cloud platform, third-party controls and network programmability.
The increased cost can be significant, depending on the scope of the deployment and the vendor chosen. The increased cost includes license fees for software and support costs. It will also cost more to support and operate this solution over time, due to complexity and software licensing.

Physical Security Stack at a Colocation Hub

For organizations that require subsecond failover and very high bandwidth, and where cloud-native controls are deemed insufficient, a physical appliance deployed in a colocation hub design may be appropriate. A colocation hub is a third-party colocation facility that is often physically adjacent to a cloud provider’s physical data center. The client organization rents rack space and connectivity from the colocation hub provider and then installs physical security appliances and a switch fabric. External connections from the public internet are routed through this edge security stack and then connected directly to workloads hosted in the public cloud provider’s IaaS or platform as a service (PaaS) platform. East/west traffic inside the public cloud VPCs is segmented by cloud-native NSGs or identity-based segmentation controls.

Figure 4 shows the physical security stack at a colocation hub design.
The main strengths of the colocation hub design are:

- High levels of security policy granularity and efficacy, similar to the virtual appliance option.
- A highly redundant design with subsecond failover and failback.
- Support for very high bandwidth.
- Maintenance and use of existing skill sets.
- A common management platform for cloud and on-premises security solutions.
- No latency penalty, in contrast to the other designs, and a superior latency profile, compared with frontending the cloud workloads with an existing data center security stack.

NSG = network security group; VPC = virtual private cloud
The main weaknesses of the colocation hub design are:

- It is not cloud-native, and therefore it is much harder to automate.
- Increased cost.
- Limited geographic scalability.

The colocation hub approach can be thought of as extending an on-premises security stack to the cloud edge. Traditional on-premises security stacks can be automated and may be part of a CI/CD pipeline, but this requires an orchestrator of orchestrators, because one cannot automate security policy inside a cloud-native framework, such as Azure Resource Manager templates. Thus this design is the most difficult to fully automate.

Geographic scalability is a major issue with this design, if an organization is highly distributed. Each geographic region requires a dedicated physical security stack to ensure an acceptable user experience. If the number of regions increases, the cost can increase very quickly for hardware, software and support. This design should be considered niche. We recommend it only for organizations with compressed geographic footprints that need very high bandwidth with subsecond failover (greater than 5 Gb per second), and for those that have a strong preexisting relationship with their colocation hub partner.

**Evidence**

This research is based on Gartner client inquiry data and the author’s industry experience of designing secure cloud environments.

---

**Recommended by the Author**

Some documents may not be available as part of your current Gartner subscription.

- Best Networking Practices Inside the Public Cloud
- Forecast Analysis: Public Cloud Services, Worldwide, 1Q21 Update
- Securing the Enterprise’s New Perimeters
- Three Styles of Identity-Based Segmentation