VALTIX

TOP 5 WAYS THAT NETWORK SECURITY IS DIFFERENT IN PUBLIC CLOUDS

The Executive Summary

Most enterprises are trying to adapt network security for their apps in multiple public clouds.

While remaining a critical domain for security, there are major differences between network security on-premises and in public clouds - across architecture, infrastructure, and operations. We cover the top 5 differences discovered in customer conversations, what they mean, and provide recommendations on how to adapt. For most, after a period of adaptation, network security will be better, faster, and cheaper - but getting there will require some work. Valtix can help accelerate that work and get organizations there sooner.

Introduction: Implementing Network Security in a Multi-Cloud Environment Is a Big Change

Every technology shift requires professionals to change the way they do things. Past transitions have ranged from mild to wild, but cloud seems almost generational for enterprises. The challenge with these transitions is to retain the lessons learned from the "old way" while embracing the unique circumstances of the new environment. In other words, the discipline remains the same, but there is a new way of doing it. This is true for security in the cloud - the hard-won wisdom from 30+ years of network security is as relevant as ever, but the implementation of it must suit the new environment. Put at a personal level, the folks who say "network security is irrelevant in the cloud," are as wrong as the folks who try to transplant legacy network security tech into the cloud environment. The same vulnerabilities and exploits will be used against apps regardless of where they live. For enterprises, the move to public cloud is a sweeping transition, spawning widespread change to architecture, infrastructure, and operations. Treating any discipline in the cloud as if it were the same as the datacenter eliminates the advantages of cloud, namely agility, speed, and cost predictability/flexibility.

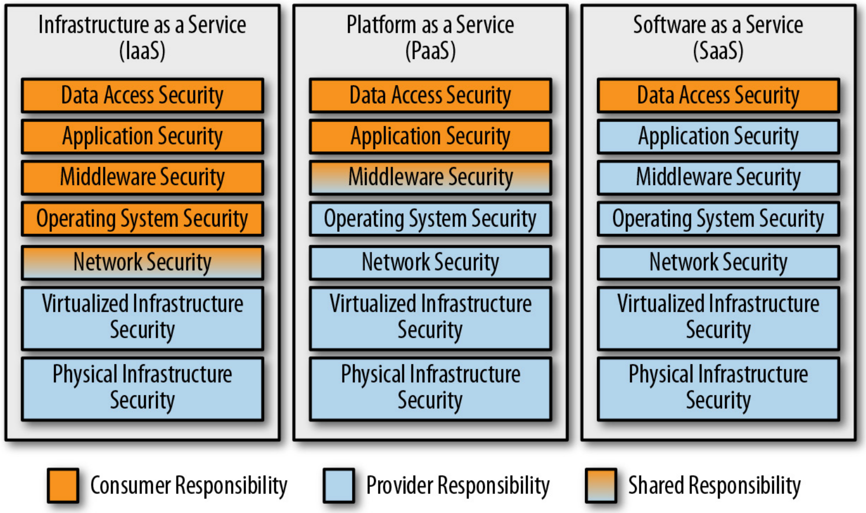
With that said, what are the biggest differences from a network security perspective? We've gathered the top 5 from various customer conversations and assembled them here. We'll try to state both what the differences are, what each means, and what can be done to address them. Let's dig in!

> *The challenge with these transitions is to retain the lessons learned from the "old way" while embracing the unique circumstances of the new environment. In other words, the discipline remains the same, but there is a new way of doing it.*

#1 End-to-end control becomes shared responsibility

The Difference:

In the datacenter, you own and control almost everything: facilities, technology, and people. But in the public cloud: You don't. You fit into the public cloud architecture and design. You don't have complete ownership and responsibility. No control over Layer 1/Layer 2 (topology/switching). From L3 onwards, you have shared responsibility. There are even things at L7 you don't have control over. You're trading off the benefits of cloud for control at various layers depending on the service. This is a good thing. This is a benefit. This is why you went to the cloud.



Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟧 Data Access Security	🟧 Data Access Security	🟧 Data Access Security
🟧 Application Security	🟧 Application Security	🟦 Application Security
🟧 Middleware Security	▨ Middleware Security	🟦 Middleware Security
🟧 Operating System Security	🟦 Operating System Security	🟦 Operating System Security
▨ Network Security	🟦 Network Security	🟦 Network Security
🟦 Virtualized Infrastructure Security	🟦 Virtualized Infrastructure Security	🟦 Virtualized Infrastructure Security
🟦 Physical Infrastructure Security	🟦 Physical Infrastructure Security	🟦 Physical Infrastructure Security

🟧 Consumer Responsibility 🟦 Provider Responsibility ▨ Shared Responsibility

Figure 1: Shared Security Model Example

What it Means:

The new reality is a shared security model (see Figure 1 for an example). This is an important change - while the business remains responsible and accountable for 100% of its initiatives and implementation, it doesn't have control over certain aspects of the cloud. It must rely on the cloud provider to help meet security requirements. The legal and regulatory implications are beyond our scope, but mitigation measures may eventually impact the technical side. But for outages and overall accountability, the business will often look to technology teams, despite the fact that those teams don't have control over much of the cloud foundation. On the networking front, L3 and up are within the tenant's purview. There are, however, differences with PaaS services - the shared security/control model changes slightly with each PaaS - each has its own model and some draw the lines quite differently (see Figure 1). Also, recent vulnerabilities in cloud services have shown that the lines of responsibility shown in this model are not as exact. For example, some PaaS offerings have had network security vulnerabilities. While these are seen as the cloud provider's responsibility, security leaders need to consider them as part of their threat modeling and attack surface considerations.

You're trading off the benefits of cloud for control at various layers depending on the service. This is a good thing. This is a benefit. This is why you went to the cloud.

#2 Change control becomes continuous change

The Difference:

In the datacenter, the traditional model of change control was highly managed infrastructure change with multiple layers of approval - e.g., 2-4 week lead times, specific change windows in the calendar, and no-change windows at certain points of the business cycle. In the public cloud, the new model is constant or, more correctly, continuous change. Application developers and DevOps all want a continuous integration/continuous deployment (CI/CD) model to deliver agile deployment of apps (a big reason why cloud is being adopted). How does security adapt to protecting the applications and meeting compliance requirements without slowing them down?

What it Means:

For many organizations, the initial forays into public cloud were pretty decentralized. As organizations became more dependent on cloud-based apps, they have tended to re-centralize management and control to ensure greater reliability and compliance. Unfortunately for some, the next reaction was to apply datacenter-style control back to the cloud. This arrests cloud benefits like agility and speed/time to market. But, it is easier to secure a static (or at least change-controlled) environment. The ideal situation is to have guardrails and traffic lights - decentralized change within standards, specific practices, and audit - enabling all of the cloud benefits, but ensuring compliance, security, reliability, and availability. But that's often hard to provide when organizations perceive an either/or choice. Forward-looking organizations are baking network security into their Infrastructure as Code (IaC) processes rather than relying on manual processes for deployment, security policy creation, and change control.

#3 Ubiquitous visibility on-prem doesn't yet exist in the cloud, even though the cloud was born instrumented

The Difference:

Visibility is always a hot topic, regardless of the domain. In the datacenter, visibility of architecture, infrastructure, and how the environment is configured is well understood - you planned, built, and configured it. In the public cloud, with rapid change and decentralized control, the environment can be much more fluid. This highlights a new need - visibility of what the environment is. However, the key component of visibility for network security always has been more around what's happening in the environment - which is a completely different discipline. See Figure 2 for more detail. While the principles of monitoring what's happening in the cloud environment are the same as they were in the datacenter, the way it's implemented will be different. So there are two kinds of visibility, one is new (what is), and the other is different (what's happening).

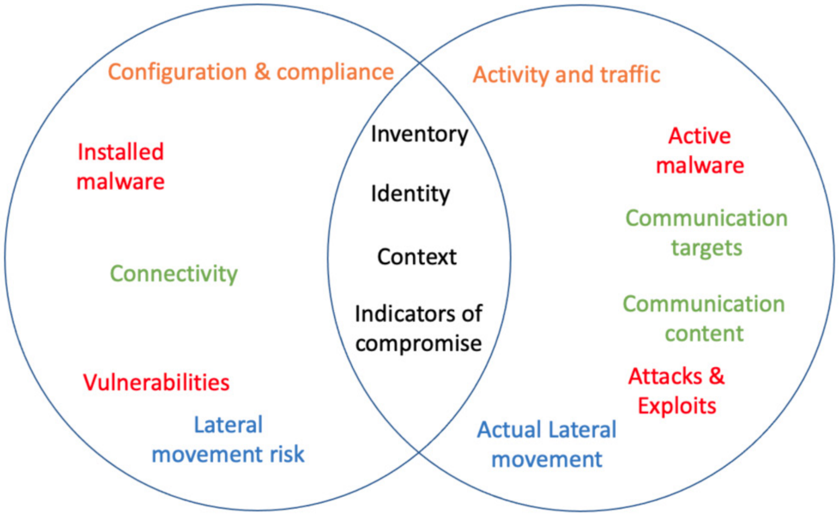


Figure 2: Two Different Kinds of Visibility

What it Means:

Options for security visibility in the cloud are expanding rapidly and are maturing, but confusion reigns and swim lanes are still being defined. Clearly, posture management tools are focused on the "what is" part of visibility as organizations work to gain a better understanding. Regarding the "what's happening" type of visibility, which has typically been the realm of various monitoring tools (IDS/IPS, event logs, SIEM, SOAR, etc.), there are some new requirements - one cannot simply be in line everywhere and look at packets (see #1 above). So while deep packet inspection will work in some places, it must be augmented, with other sources - e.g., cloud DNS logs, VPC flow logs, cloud API logs, and workload context (dev, test, prod, compliance). While SIEMs can synthesize and correlate information well, some information must come from original sources. For example, it's not possible to derive workload context or instance information days after an attack purely based on ephemeral IP addresses in traffic logs of a dynamic, auto-scaling workload. And organizations must address the learning curve from these new sources of information as well - they are often richer but must be handled differently.

#4 Appliances are obsolete

The Difference:

Yes, really. You don't have to manage appliances anymore! You're not installing and configuring boxes. Boxes are a busted management model in the cloud, and this was rapidly understood in many disciplines (compute, storage, networking). But because security appliances are so feature-rich and powerful, there is a bit more reluctance to let them go, and sometimes we are perpetuating older designs such as active-passive high availability and large throughput boxes instead of horizontal auto scaling. Yet you still have requirements to do everything the boxes did for you in the datacenter: prevention, protection, visibility, monitoring, etc.

> *But no more boxes = no more management headaches. This is a new way of doing things, where a service-based network security infrastructure manages its own enforcement points.*

What it Means:

Firewalling still matters. You still have vulnerabilities, attacks, threats, configurations. These require defense-in-depth. You have regulatory and risk management compliance. Many organizations have hard-coded policies naming firewalls and other network security functions that have been approved by the board. Firewalling still matters, even if firewalls don't - because appliances, even virtual ones, have no fit in the cloud model. Everything in the cloud - compute, network, storage, database, etc. - is delivered and managed as a service, where the management of instances of that service is part of the service. In other words, infrastructure manages itself, leaving admins to focus on policies. Anything that requires operations teams to manage individual boxes will ultimately be rejected because it's an archaic model in an environment where there are service-based alternatives. But no more boxes = no more management headaches. This is a new way of doing things, where a service-based network security infrastructure manages its own enforcement points.

#5 De facto standards-based architecture gives way to proprietary clouds

The Difference:

In the datacenter, you could pick whatever product you wanted for infrastructure, operations, security, etc. They all complied with some standards or well known architecture patterns. There would be interoperability. Sure, there were implementations that differentiated themselves based on tighter integration, but for the most part, products HAD to work together; else they weren't around very long. While there are seemingly similar services at each cloud provider for every feature/function, implementing the same application to be multi-cloud is not a practical reality. Essentially, in the cloud, everything is proprietary to the provider (see Figure 3).

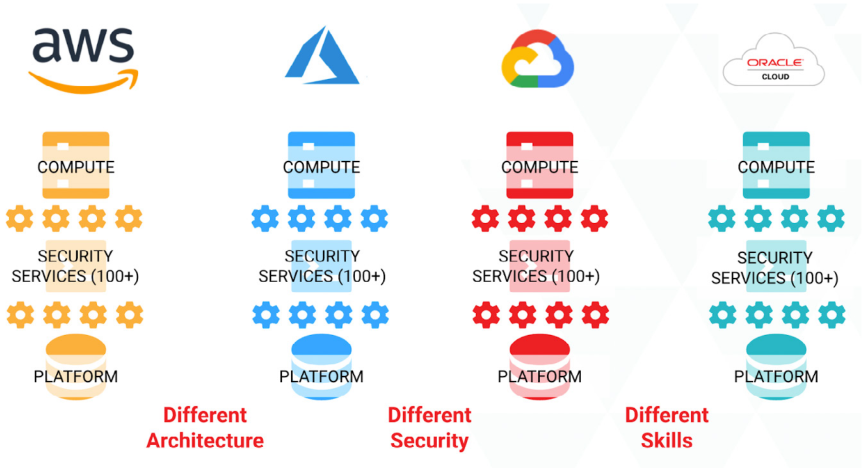


Figure 3: Each Cloud Has Its Own Implementation of Almost Everything

What it Means:

The organization has to make a decision - use proprietary services bound to the cloud provider and manage each cloud as a silo? Another way to look at it - do you want to be locked in or not? For many application services, it doesn't matter. But when organizations need an enterprise-wide, multi-cloud perspective (like one would with security), there may be issues with this approach. All of this, of course, assumes that organizations are multi-cloud - that's another decision that may or may not be on the table, as many organizations find themselves multi-cloud already. Silo and lock-in issues aside, it's important to remember that cloud providers have a security service to get you on the platform - they check a box. It's usually well-integrated into the infrastructure, but they are not in the business of providing the best security.

Recommendations

Those are the Top 5 differences we've seen enterprises adapting to.

Forward-leaning organizations have used the hard-earned knowledge of enterprise network security and all of the lessons learned protecting apps in the datacenter, but with new technologies and operations models. At a more detailed level:

- Nobody is going to change the cloud - shared responsibility and proprietary cloud implementations are here to stay. Risk management, legal, and regulatory compliance will catch up, but network security folks will have to contend with this reality in both their processes and their toolsets.
- Change management/guidelines are better for business than change control. Learn to govern and secure in that mindset. Leverage IaC to bake security into DevOps processes. In terms of guiding change, this emphasizes visibility more than control. In terms of coping with change, defense-in-depth and controls that adapt to workload context become far more important than when organizations could slow change down and count on a static environment to secure.
- Modern security + modern ops model = cloud benefits with security. There are implications for every security discipline, but particularly for visibility, protection, prevention. Missing either good security or cloud ops is a recipe for failure.

Forward-leaning organizations have used the hard-earned knowledge of enterprise network security

The Top 5 Differences: Some Make NetSec Harder, Some Make It Easier - All Require Some Change

Long term, most of these differences will make network security easier. But they will all require some change. Valtix is focused on multi-cloud network security and can help organizations adapt their security processes to the cloud faster. By delivering a set of services that exceed enterprise expectations on network security while fitting into the cloud ops model, Valtix enables organizations to transcend these differences and retain both enterprise network security and cloud benefits.

#1	**End-to-end control becomes shared responsibility**	**Simplify L3-7 Security** As a cloud-native service that integrates with constructs in each cloud, Valtix enables visibility and control in a workload context, which is what most enterprises care about.
#2	**Change control becomes continuous change**	**Dynamic Multi-Cloud Policy** Since Valtix is a cloud-native service, and integrates with cloud constructs, it understands both the dynamic environment and workload identity and context, and can adjust both enforcement points and policies automatically.
#3	**Ubiquitous visibility on prem doesn't yet exist in the cloud, even though the cloud was born instrumented**	**Continuous Visibility and Discovery** With both traditional network visibility and native cloud instrumentation, Valtix provides complete visibility of what's happening from a security perspective in your cloud environment.
#4	**Appliances are obsolete**	**Security-as-a-Service** Valtix delivers multi-cloud security as a service - taking advantage of all of the benefits of cloud while fitting into the modern operations model.
#5	**De facto standards-based architecture gives way to proprietary clouds**	**Multi-Cloud, Multi-Account** Valtix's multi-cloud network security enables organizations to bridge proprietary cloud siloes with a single dynamic policy to protect in the top public clouds.

VALTIX

VALTIX IS ON A MISSION TO ENABLE ORGANIZATIONS WITH SECURITY AT THE SPEED OF THE CLOUD.

Deployable in just 5 minutes, Valtix was built to combine robust multi-cloud security with cloud-first simplicity and on-demand scale. *Powered by a cloud-native architecture, Valtix provides an innovative approach to cloud security called Dynamic Multi-Cloud Policy™, which links continuous visibility with advanced control. The result: security that is more effective, adaptable to change, and aligned to cloud agility requirements. With Valtix, organizations don't have to compromise in the cloud. They can meet critical security and compliance requirements without inhibiting the speed of the business. Valtix has been recognized as an innovator in numerous industry awards including 2021 top honors in the "Next-Gen in Cloud Security" from Cyber Defense Magazine, SINET-16 Innovator recognition, and inclusion in Gartner's Cool Vendors in Cloud Networking report.*

Get started today with our Free Tier at **Valtix.com**.

HQ - Santa Clara, USA
2350 Mission College Blvd #800 Santa Clara, CA 95054
650.420.6014 info@valtix.com