

**TAG CYBER**

**THE NEED FOR  
MULTI-CLOUD  
SECURITY IN THE  
MODERN ENTERPRISE:  
AN OVERVIEW OF THE  
VALTIX PLATFORM**

EDWARD AMOROSO, TAG CYBER



# THE NEED FOR MULTI-CLOUD SECURITY IN THE MODERN ENTERPRISE: AN OVERVIEW OF THE VALTIX PLATFORM

EDWARD AMOROSO

---

The modern CISO must balance available new security controls offered by the major cloud providers with the need to secure increasing multi-cloud use across the enterprise. An integrated multi-cloud security platform is the recommended approach, and the Valtix<sup>1</sup> platform offers an effective commercial implementation.

## INTRODUCTION

The chief information security officer (CISO) is presented today with a challenge regarding multi-cloud security: On the one hand, they are being approached by each of the major cloud providers touting embedded cyber security controls. Through acquisitions such as Microsoft's recent purchase of CloudKnox,<sup>2</sup> or through natively developed controls such as AWS Cognito,<sup>3</sup> cloud providers offer increasingly effective means for protecting the workloads that they host. Still, for regulated industries, some might find the native protections insufficient.




On the other hand, CISOs must also contend with increased use of multiple cloud and software as a service (SaaS) tools across the business units being supported. Recent surveys<sup>4</sup> (as well as our own research — see below) confirm that multi-cloud has become the new normal for most enterprise teams. These insights imply that despite efforts from cloud providers to encourage consolidation to a single cloud, this is not likely to occur in most enterprise IT contexts.

As a result, CISOs must find a healthy balance between the security solutions being offered by cloud providers and the multi-cloud needs of the businesses being supported. Such balance must begin with the initial architectural design and must extend into day-to-day security operations. It must also incorporate the need to keep up with a massively changing threat model from capable malicious actors, including nation-states.

In this report, we make the case for an integrated multi-cloud security platform. We make our case with emphasis on the need to include strong network security to protect application workloads hosted in each cloud provider. This should be evident, since the network comprises the basic fabric that ties together multiple cloud infrastructures into a coherent architecture. The commercial Valtix platform is used to illustrate this multi-cloud network security approach for enterprise deployments.

## SECURITY OFFERINGS FROM MAJOR CLOUD PROVIDERS

The major cloud providers have obviously recognized the importance of cyber security for their customers. While each will certainly acknowledge the likelihood that multi-cloud usage will be practiced by their customers, they have not moved in the direction of standard, common, unified protections for their various competing services. These differences are apparent just in the naming used for frequently cited functional requirements from the providers (see below).<sup>5</sup>

<b>Compute</b>	Elastic Cloud Compute (EC2)	Virtual Machines	Compute Engines
<b>App Hosting</b>	Elastic Beanstalk	Cloud Services	App Engine
<b>Serverless</b>	AWS Lambda	Azure Functions	Cloud Functions
<b>Container</b>	ECS/EKS Containers	AKS Container	Kubernetes Engine
<b>Storage (File)</b>	S3 Storage	Azure Storage	Cloud Storage
<b>Storage (Block)</b>	Elastic Block Storage	Azure Blob	Persistent Disc
<b>Backup</b>	AWS Glacier	Azure Backup	Cloud Storage
<b>Orchestration</b>	Data Pipeline	Data Factory	Cloud Dataflow
<b>Management</b>	AWS Redshift	SQL Data Warehouse	Google BigQuery
<b>NoSQL DB</b>	AWS DynamoDB	Cosmos DB	Cloud Datastore

**Figure 1. Inconsistent Function References From Major Cloud Providers**

As one would expect, the inconsistencies across the major cloud providers extend to their provision of security capabilities. Container security, orchestration, and visibility are all performed using unique methods across major cloud infrastructure, so modern CISOs and their teams must contend with this disparate approach, which is exacerbated by the increased use of multi-cloud.

## MULTI-CLOUD USAGE IN ENTERPRISE

It was referenced earlier that research indicates increased use of multi-cloud by enterprise. While this is not an unexpected result, we confirmed this trend through a minisurvey of various cyber security practitioners. We asked them a simple question — namely, whether multi-cloud usage in their enterprise (and we agreed to maintain confidentiality in their responses)<sup>6</sup> was likely to increase, decrease, or stay the same.

The result of our minisurvey, which included 12 practitioners with responsibilities directly or indirectly related to cloud security across a variety of business sectors, was that half of those asked (six) reported present or future increased multi-cloud use. One third of those asked (four) responded that that multi-cloud usage would roughly stay the same. Two the practitioners asked this question reported an expected reduction in multi-cloud use.

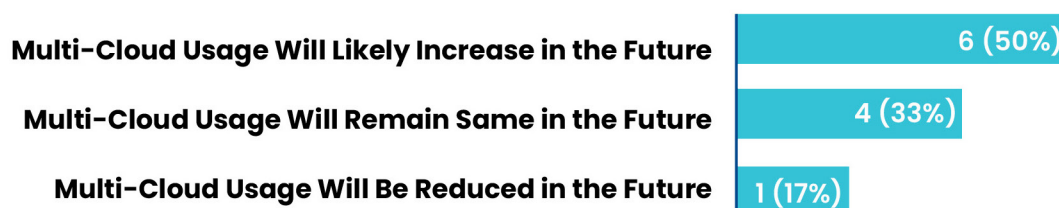


Figure 2. Results of Minisurvey for Multi-Cloud Use

While the size of the minisurvey was small, its result is consistent with many other surveys, including the HashiCorp report cited earlier. It should be therefore accurate to conclude with some confidence that most enterprise security teams will have to deal with security threats and compliance issues for multiple cloud offerings (with their many inconsistent security controls) for years to come.

## REQUIREMENTS FOR INTEGRATED MULTI-CLOUD SECURITY

The need thus arises for enterprise security teams to identify and implement an integrated security and compliance solution for their multi-cloud infrastructure. Obviously, such capability must integrate with select security controls implemented by the cloud providers, but it requires the introduction of new platform capabilities that can deal with the great challenges associated with the use of different cloud services.

The requirements for an integrated platform will include functional capabilities for real-time protection, interface support to support connection with internal and external environments, and reporting functions to support governance, compliance, and oversight. By identifying these requirements, security teams can streamline the selection of a suitable commercial platform to help support this goal of integrated protection.

To define an effective set of security requirements for modern cloud-hosted applications and services, it is helpful to first review the actual threats that will exist in these new virtual environments. With the transition to cloud, application owners lose any semblance of security protection that legacy firewall perimeters might have offered — however inadequate some components might have been.

Threats to cloud applications and services track the familiar taxonomy of cybersecurity issues for any online asset. This includes the CIA triad<sup>7</sup> — confidentiality, integrity, and availability — as well as fraud issues for cloud services that include e-Commerce-based handling of payments. This implies that despite service-level agreements with cloud service providers, this aspect of the enterprise is not immune to the cyber risks that enterprise teams have addressed for years.

To address these threats, several excellent controls have emerged that provide a basis for reducing the cyber risks associated with cloud-hosted application and services. These controls are listed below, 12 in total, that serve the dual role of helping to explain the nature of world-class security protection in cloud and serving as a useful basis for source selection of a suitable cloud-native security platform.

- *Agentless Support for Multi-Cloud* – It is generally helpful to reduce the agent footprint across any security deployment. Additionally, not every application architecture allows agent-based security (serverless), thus creating fragmented security policy management. Security support for multi-cloud that can be done without having to install and manage a software agent is therefore desired.
- *Application Discovery* – The requirement to identify and discover the applications that are hosted and supported in a multi-cloud environment is important, especially in environments where unmanaged apps are common.
- *Automated Security Provisioning* – Ultimately, the purpose of multi-cloud infrastructure is to streamline the provisioning of computing resources. To that end, security controls should be easily provisioned using automated tools.
- *Continuous Visibility of Egress Traffic* – Visibility of traffic leaving multi-cloud apps and services is an important means for identifying any data leakage risks. This should be done in a manner that maximizes the ability to view both content and metadata.
- *Data Plane Attention* – Most cloud infrastructure is partitioned and separated into data and control planes. Including security controls for data plane traffic is therefore required to avoid leakage, modification, or blocking.
- *Deep Packet Inspection* – To provide for protection coverage of network activity into and out of the multiple clouds, it is helpful to have access to deep packet inspection (DPI) tools that support collection and analysis by security experts.
- *Global Policy Management* – Reference to global policy in this context involves cyber security decisions about each commercial cloud being used, as well as any legacy or hybrid infrastructure or services.
- *Lateral Movement Control* – Addressing lateral movement is one of the primary tenets in reducing the incidence and risk of advanced persistent threats (APTs). Past incidents involving nation-state actors always included some lateral movement.
- *Multi-Cloud Integration* – Integration of multi-cloud infrastructure protections is essential for avoiding any policy control gaps that might exist at the seams between commercial clouds.
- *Next-Generation Firewall* – Next-generation firewall (NGFW) capability is important to maintain domain boundaries and appropriately segmented applications in the cloud.
- *Protection From Inbound Threats* – Just like outbound threats, the avoidance of inbound threats is a critically important element of cloud security, including reducing the risk of ransomware, APTs, and other threat campaigns.
- *Scalable Infrastructure* – The security tools, systems, and infrastructure used in multi-cloud must be scalable, since the basic purpose of any cloud capability is to handle extensibility and expansion without intervention.

Many other conventional protection requirements will exist to help secure multi-cloud services. For example, multi-factor authentication, log management, and least privilege for system administrators are all examples of canonical security controls present in virtually all computing environments. The requirements listed above are ones that introduce unique control capabilities for multi-cloud that might not be supported by other controls.

## VALTIX PLATFORM OVERVIEW

Led by industry veteran Douglas Murray, Santa Clara, California—based Valtix provides an integrated multi-cloud network security solution delivered as a service to secure enterprise workloads. The features of the platform provide an excellent case study for the requirements described above. Valtix customers are focused on creating an integrated means for establishing a balance between the multi-cloud needs of the organization and the security features offered in each cloud service.

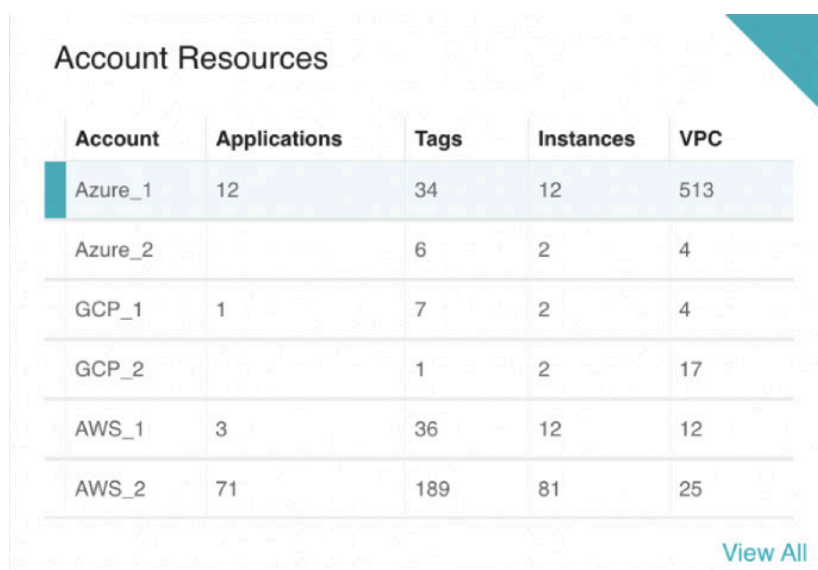
The solution is based on a technology known as Dynamic Multi-Cloud Policy, which is designed specifically to adapt quickly as the configuration and usage of a customer's multi-cloud infrastructure changes. This allows enterprise security teams to define one set of security policy controls that can apply to many clouds. This also allows for more effective compliance processes and framework mappings, such as to NIST 800-53.<sup>8</sup>

### *Valtix Visibility*

The platform includes capability to provide continuous discovery of cloud assets and cloud applications identities. Such visibility is implemented through a three-step cloud account process of (1) discovery, where cloud assets are identified and reviewed for security gaps, (2) deployment, where security protection is installed via the Valtix console, and (3) defense, where the network security is configurable according to on performance or other considerations. As a whole, Valtix provides layers of visibility that span assets, network security posture, traffic flow (e.g., DNS, VPC flow, and inspection of ingress, egress, and East-West traffic), and threats (e.g., exploits, malware, web attacks, exfiltration, and malicious site attacks).

### *Valtix Control*

The platform includes support for fine-grained, cloud-aware policy enforcement based on asset and application identity discovery. Security administrators are offered real-time views into their accounts, tags, and instances for popular cloud services such as Microsoft Azure, Google Cloud Platform (GCP), and Amazon Web Services. These account resources can be assessed with respect to the organization's common policy rule definitions.



Account	Applications	Tags	Instances	VPC
Azure_1	12	34	12	513
Azure_2		6	2	4
GCP_1	1	7	2	4
GCP_2		1	2	17
AWS_1	3	36	12	12
AWS_2	71	189	81	25

[View All](#)

Figure 3. Typical Console for Multi-Cloud Account Resource Visibility



Security teams that are struggling with the challenge of multi-cloud will benefit from the use of a commercial tool that helps to unify policy controls and offer an integrated means for supporting the concurrent use of multiple cloud solutions with nonstandard (and even competing) capabilities. The Valtix platform provides such support via a commercially available solution that can be installed and managed without great complication or effort.

## SUMMARY RECOMMENDATION

The bottom-line recommendation regarding both multi-cloud security in the modern enterprise and the Valtix platform is as follows: Organizations should take inventory of their multi-cloud strategy and how it relates to cyber risk. They should then deploy a commercial solution that can make the management of different types of applications on different public clouds simpler and more secure.

## ABOUT TAG CYBER

TAG Cyber is a trusted cyber security research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and nonclients alike — all from a former practitioner perspective.

<sup>1</sup> <https://valtix.com/>

<sup>2</sup> <https://blogs.microsoft.com/blog/2021/07/21/microsoft-acquires-cloudknox-security-to-offer-unified-privileged-access-and-cloud-entitlement-management/>

<sup>3</sup> <https://aws.amazon.com/cognito/>

<sup>4</sup> See the multi-cloud usage survey from HashiCorp: <https://virtualizationreview.com/articles/2021/08/12/multi-cloud-survey.aspx#:~:text=In%20announcing%20the%20survey%20report,do%20so%20within%20two%20years.>

<sup>5</sup> References to functions for the major cloud providers are taken primarily from marketing materials available on their public websites and available product brochures and white papers.

<sup>6</sup> Our data research methodology at TAG Cyber includes several means for gathering data. We operate the NYU CCS index, for example, which includes monthly queries to practitioners (all confidentially reported) on topics related to cyber security. We share the results of these surveys publicly for researchers here: <https://wp.nyu.edu/awml/>. We also engage directly with CISOs and other practitioners on a regular basis as part of our analyst and consulting work. We frequently use these interactions to query these practitioners on issues such as multi-cloud use. We believe this research approach to be superior to the more commonly found method of emailing a large group of people who have been paid by research firms to respond to such surveys. Unlike more academic research, however, responders are generally quite uncomfortable providing their names for inclusion in the research, often to the proprietary nature of their work and the desire by their legal staff to avoid making any types of public claims related to security.

<sup>7</sup> An acceptable description of the CIA model is available at <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA#:~:text=Confidentiality%2C%20integrity%20and%20availability%2C%20also,with%20the%20Central%20Intelligence%20Agency.>

<sup>8</sup> <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>