



## **WHY VALTIX**

Security at the Speed  
of the Cloud

# The Cloud Era Has Begun. Network Security Must Adapt.

The requirements of security are changing once again. Decades ago, organizations moved from mainframes to servers. In the process, a model of security emerged that relied on well-architected networks, firewalls, DMZs, and a variety of system-level and application-level security controls. Today, more and more organizations are making yet another move.

According to Gartner, "By 2023, 40% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 20% in 2020." According to IDC, public cloud spending accelerated by 34%, and non-cloud IT infrastructure declined by almost 9% in 2020.

Across every industry, many organizations are now taking a "cloud-first" approach. These organizations adopt a cloud-first mentality in order to enable greater business agility, which results in a competitive business advantage. As they make the move, the number one challenge

for these organizations: how do they maintain resilience and security, while fulfilling the business's need for agility and speed?

Cloud-first organizations know that legacy on-prem tools can hold them back in the cloud. On-prem tools weren't built around cloud assumptions. Cloud-first architecture starts with a blank sheet of paper with the intent of building for the next decade, not the last.

And when it comes to security, Cloud-first teams realize that security in the cloud must be architected around a more dynamic environment. They know that failing to do so will result in security gaps that lead to costly remediations or even worse, business-impacting security breaches. At the same time, Cloud-first teams expect that security should just work and shouldn't slow down delivery for the business. Security technology must move with the same agility as the cloud apps it supports.

*By 2023, 40% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 20% in 2020* -Gartner

# Cloud teams need a Cloud Network Security Platform (CNSP)



To address the needs of cloud teams, new breeds of security technology are emerging such as Cloud Security Posture Management (CSPM), Cloud Access Security Broker (CASB), and Cloud Workload Protection Platforms (CWPP). For network security, which remains critical to overall security architecture, a Cloud Network Security Platform (CNSP) is becoming a requirement. A CNSP must deliver on three key capabilities: Visibility into dynamic cloud assets and network telemetry; Multi-cloud security through a single console; and Cloud-native scale to enable business agility.

## Visibility into Dynamic Cloud Assets and Network Telemetry

There is no security without visibility. Long advocated by key cybersecurity frameworks such as NIST and CIS, security teams know that you have to start with identifying assets. Asset identification should include context and understanding of the business purpose of the resource in order to apply risk-based policy and the appropriate security controls.

Cloud architecture challenges this basic practice when multiple teams, apps, and business-aligned projects introduce change continuously. Additionally, important visibility into security telemetries such as VPC flows and DNS logs are locked within cloud-provider-specific systems. And with constant change as the norm, visibility solutions that rely on scanning or agents fail to live up to their promise.

By capturing visibility through the network across many disparate teams, applications, and cloud providers, a CNSP provides better visibility for security that is continuous by design. Through a CNSP, visibility into network telemetry from the cloud provider is unlocked and then enriched with threat intelligence and/or exported to a SIEM. Operations teams benefit as well with an updated source of truth about the key applications and assets across multiple cloud accounts and virtual networks.

## Multi-cloud Security Through a Single Console

No organization wants to be locked into one cloud. According to Gartner, 81% of respondents say they are working with two or more cloud providers. Beyond the obvious issue of vendor lockin, a single cloud strategy threatens business resilience through dependence on one provider who may suffer an outage.

Despite the obvious issues of a single-cloud strategy, many of the same organizations who cite a desire to pursue multi-cloud, still act like single cloud consumers. They adopt a single-cloud mentality because it is convenient. They adopt a single-cloud mindset for security because they don't believe multi-cloud tools exist to give them the enterprise security they require. Instead, they choose to build for a single-cloud architecture that they must replicate for each cloud provider they adopt. No cloud or security team should accept a single-cloud mindset.


A CNSP provides an abstraction layer that simplifies multi-cloud security. Through a CNSP, security teams gain the ability to apply one policy that can span multiple clouds. Operations teams benefit from reducing the need to maintain cloud provider-specific infrastructure and a reduction in overall cloud provider lockin.

## Cloud-native Scale to Enable Business Agility

Security only works if it can adapt to the scale of the resources it's meant to protect. According to Gartner, by 2025 99% of cloud security failures will be the customer's fault. With Cloud infrastructure (IaaS), the shared responsibility model makes everything beyond physical security the customer's responsibility, which introduces the challenge of orchestrating and automating security tools across the public cloud. It's especially challenging when the security tools being orchestrated were meant for the different assumptions of the data center and on-prem infrastructure. And stitching together a patchwork of legacy technology leads to costly maintenance and inevitable failures.

A CNSP should deliver security that just works and is seamless to the cloud apps it protects. It should be enabled through infrastructure as code (IaC) tools like Terraform. New apps and infrastructure should be continuously discovered and security policy automatically deployed based on the technology asset's business context. Elasticity should occur as consumption happens and business demand requires it. Security in the cloud should just work – thus enabling teams to focus on security and not operating the tools.

# Meet the Valtix Cloud Network Security Platform.



Valtix is the industry's first Multi-Cloud Network Security Platform delivered as a service. Only Valtix provides robust cloud network security at the speed of the cloud.

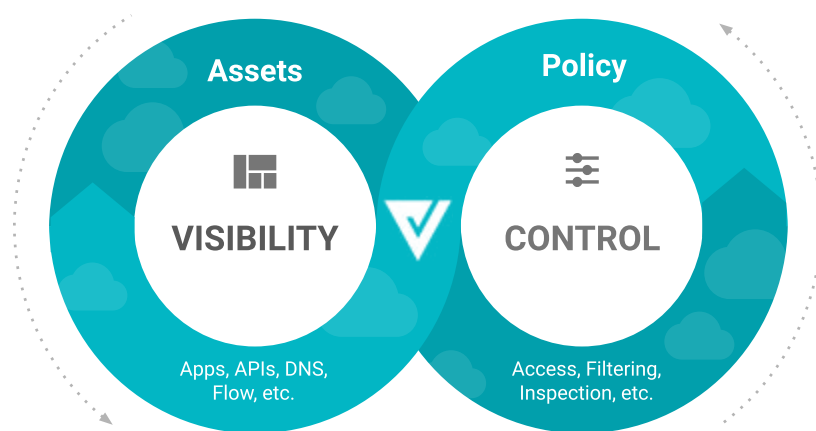
With Valtix, cloud operations and security teams can gain:

- **Robust Security, Cloud-first Simplicity.** Achieve robust cloud security through advanced security controls such as firewall, web application firewall (WAF), DLP, and IDS/IPS that are simple to deploy and manage.
- **Continuous Visibility.** Enable dynamic policy through continuous, real time visibility of apps and infrastructure & unlock network telemetry for DNS and VPC Flow.
- **One Policy, Many Clouds.** Consolidate network security management in one console, through a single dynamic policy framework across accounts, virtual networks, cloud providers.
- **On-demand Scale.** Adapt continuously to changes, new assets, and scale security on-demand as the business requires it through alignment with cloud automation best practices and infrastructure as code (IAC).
- **End-to-end Platform.** Eliminate the need for cloud network security point solutions and simplify practitioner workflow by consolidating on a single platform for cloud network security.

## A Powerful Approach to Cloud Security: Valtix Dynamic Multi-Cloud Policy™

For security teams, Valtix provides a cloud-native security model called the Valtix Dynamic Multi-Cloud Policy. This approach ties together continuous visibility and control to discover new cloud assets and changes, associate tag-based business context (from cloud provider), and automatically apply the appropriate policy to ensure security compliance.

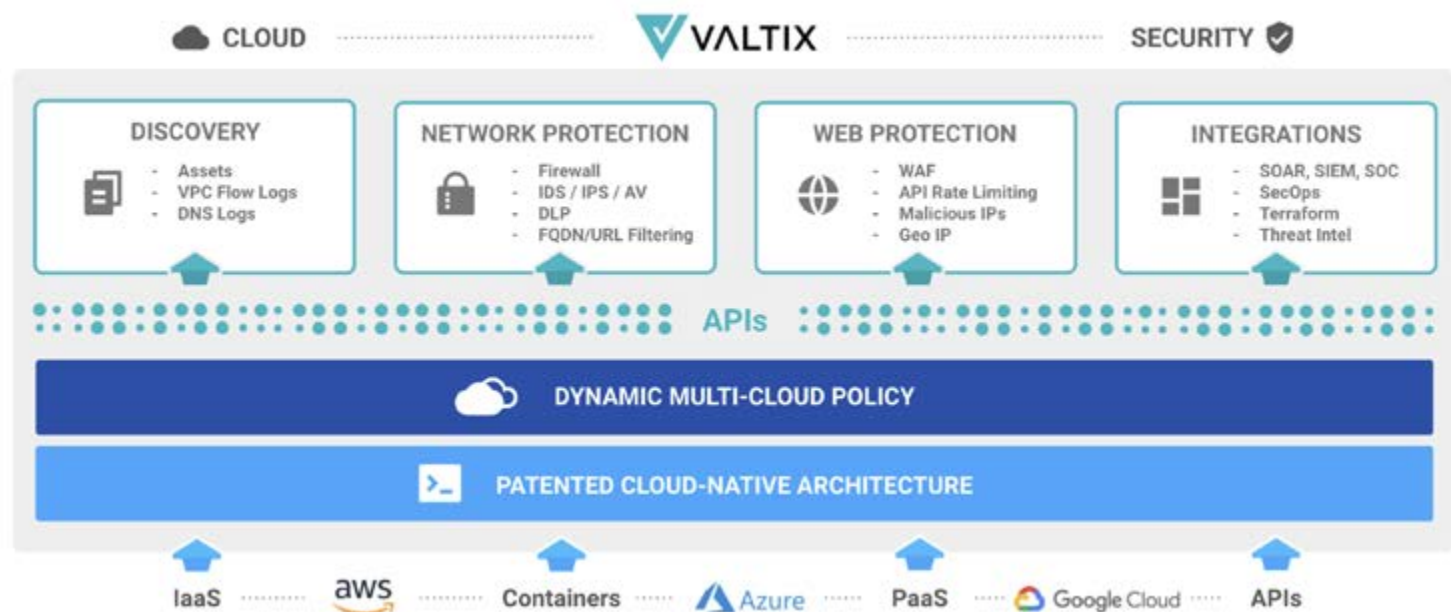
Once configured, the net result of Dynamic Multi-Cloud Policy is security infrastructure that just works and remains invisible to cloud teams responsible for their deployments. Dynamic Multi-Cloud Policy helps ensure that critical security gaps don't emerge and that the business stays secure and resilient. This is a key innovation that is unique to Valtix.



## Provides an End-to-End, Open Platform for Cloud Network Security

Additionally, Valtix adheres to the principles and best practices of leading security platforms. The Valtix platform was built for maximum flexibility, extensibility, and addresses a number of security use cases including asset discovery, network-based security, web application security, and integration of security event telemetry into data stores such as Splunk.

Valtix makes use of an ecosystem of capabilities such as threat intelligence feeds, third-party antivirus, and malware signatures. Valtix is open, providing API level access (future) to extend its usage further. The possibilities are endless, as the open approach of Valtix can be applied (future) to third-party and cloud-provider-specific security controls.



## Powered by a Patented Cloud-Native Architecture

The Valtix platform is powered by a patented architecture that is cloud-native and borrows from best practices of software-defined networks to achieve on-demand scale. By decoupling the data plane from the control plane, the platform ensures security data stays within the customer's cloud accounts, thus adhering to compliance regulations. At the same time, the Valtix platform can be centrally controlled and managed through a single cloud-based console. Valtix scales on demand because the architecture utilizes native cloud provider capabilities, integration with cloud automation tools like Terraform, and architectural best practices to add additional capacity as it's required.

Another innovation of the architecture, Valtix Single-pass Pipeline (™) enables 10x throughput and latency improvement over other solutions. But just as importantly, Single-pass Pipeline enables a variety of application architectures, cloud network structures, and the use of platform services such as AWS S3 or serverless infrastructure. It also enables the Valtix Platform to consolidate multiple traditionally siloed point products for network security into a single solution.

## Elastic Consumption Aligns with Dynamic Needs

For cloud executives and budget owners, the Valtix platform provides a better economic model for dynamic cloud requirements. Competing approaches either leverage complex and fragmented models of pricing or maximum capacity-based on-prem models of licensing.

## The Valtix Mission: Security at the Speed of the Cloud

Valtix provides a new model of security built on the cloud, for the cloud. Valtix provides continuous visibility and advanced control to centrally secure apps across providers, virtual networks, and DevOps teams. Valtix is the future of network security for cloud infrastructure and the apps that run there.

Because it is dynamic, invisible, and aligns to cloud agility requirements, Valtix delivers on its mission of security at the speed of the cloud.

*Get started with a free trial and a cloud visibility report at [Valtix.com](https://www.valtix.com)*





## WHY VALTIX

Security at the Speed  
of the Cloud

HQ - Santa Clara, USA  
800# Mission College Blvd 2350  
95054 Santa Clara, CA  
650.420.6014  
[info@valtix.com](mailto:info@valtix.com)