VALTIX

THE ESSENTIAL GUIDE TO CLOUD NATIVE NETWORK SECURITY

WHITE PAPER

Speed of the Cloud

The cloud is naturally evolving as the new business environment. Wider adoption is inevitable—and accelerating. Yet on-premises security architectures can no longer adequately support the dynamic, elastic nature of today's (and tomorrow's) cloud. Only a native security solution can unify single and multi-cloud security for greater visibility, scalability, and performance. It's time for cloud security to move at the "speed of cloud."

Business at the Speed of the Cloud

Business competition—regardless of market, region, or customer base—has quickened its pace over the last decade and forced irrevocable change in even the most staid and stable companies and institutions. Everything from farming and manufacturing to electronics and entertainment operate at a faster 'speed of business' in a race to provide the products and services that deliver demonstrable customer value—and market advantage.

Given the pervasive role of technology in this shift, it's fair to say the speed of business is enabled by the "speed of cloud."

Companies and institutions that ignore this type of business agility risk falling behind. However, full adoption poses challenges for many companies transitioning to this more dynamic and agile cloud model. Many of these challenges are rooted in the evolution of applications and the data center infrastructure itself.

Application architectures have evolved on a steady march toward more decentralization, segmentation, and partitioning interlinked by API interfaces. This shift includes cloud-native design, micro services-based architecture, and the use of containerization. Increasingly, applications behave like services in the cloud—services that are highly redundant, scalable, and at times, transient.

In this new model of application design and structure, a new model of application development and deployment emerged. Because applications could be run in a cloud as a service and were smaller in function, they could be compiled and built more rapidly and individually than before. This trend has led to more speed and frequency of change in application deployment and has made the DevOps function more critical to achieving business agility. Moving at the speed of the cloud involves a progressive shift to continuous integration and Continuous Deployment (CI/CD) in the era of DevOps.

Un-Controlled Data Center Sprawl in the Multi-Cloud Journey

The advantages of multi-cloud and cloud-native computing are compelling, and more enterprises are embracing the shift for greater productivity, performance, and innovation. While most enterprises begin with one cloud vendor, the data is resoundingly clear, it is only a matter of time before an organization that has embraced the cloud begins using two or more clouds. In a recent Gartner survey, 81% of respondents said they are working with two or more providers.

Whether on one cloud with multiple regions and VPCs, or using multiple clouds, data center cloud sprawl has become a big issue for enterprises. Data centers no longer have a defined perimeter and have become dynamic and ever-changing with the cloud.

Several factors contribute to the emergence of data center sprawl:

- **Adoption of the cloud is highly decentralized** – like the adoption of mobile phones in the enterprise that created uncontrolled BYOD IT problems. Today application teams are comfortable setting up a VPC and using the cloud as a testing or production environment for their application. These application teams can be anywhere, making it all the more difficult for centralized security staff to be fully aware of where the cloud is being used and how.
- **App teams pick clouds based on what is best for the app** – in some cases application teams decide what cloud is best for an application, largely on factors such as in-house expertise or performance – factors that are not security-related.
- **Enterprises are going multi-cloud.** Many reasons exist for the rise in multi-cloud adoption, including the need for increased operational agility, high availability / disaster recovery strategies, and avoiding vendor lock-in.
- Disaster recovery is critical given even public clouds can have outages, such as in June 2019 when the Google Cloud Platform saw outages in the eastern US region.

> “Of the 727 cloud technology decision makers at large companies surveyed, 86% said they now have a multi-cloud strategy. And 60% of enterprises are now moving, or have already moved, mission-critical applications to the public cloud, the report found.”
>
> – *TechRepublic, March 2019*

All of these factors create a perfect storm for traditional IT and security ops. This rapid acquisition of clouds leads to a growing data center cloud problem that makes it almost impossible for security teams to have full visibility or control of the enterprise-wide cloud.

Naked and Agile or Secure and Rigid

As enterprises encounter data center cloud sprawl, it becomes very difficult for security to keep up with applications or the application teams deploying them in the cloud. According to the 2018 State of the Cloud Report from Right Scale, 77% of enterprises felt that cloud security was a significant challenge.

In this environment, it is not uncommon for security to be seen as a bottleneck to business agility in the cloud. Organizations often fall into one of two situations: being agile but naked, or rigid yet secure.

When companies are agile, they are deploying back-end infrastructure and applications quickly to the cloud and can offer new services rapidly, potentially gaining an advantage over competitors. Typically, traditional network security operations are too slow to react to these deployments, and consequently, only minimal security is put in place—often by DevOps, and often with non-approved offerings from a cloud service provider themselves. These organizations are 'naked' from a security standpoint given the weak coordination and verification of their security strategy by the owners in IT of security strategy for the organization.

On the other hand, organizations may defer to security ops to put in place adequate security controls before launching applications. This often hampers business agility, as application development teams must wait for central security operations to provision back-end services and put the appropriate security policies in place. In this case, organizations remain secure, but they are rigid and slow-moving.

One clear reason for this dichotomy is that much of cloud and traditional security IT groups feel security solutions have been lagging cloud use and innovation. In the 2018 Magic Quadrant for Next Generation Firewalls, Gartner highlighted that enterprises are seeking NGFW vendors with current SDN support or SDN in their roadmaps, including more automated firewall policy orchestration.

Furthermore, a March 2018 Survey of cloud security professionals by Dimensional Research highlighted several of the challenges in securing cloud and multi-cloud environments:

- **83%** have problems regarding next generation firewalls, including licensing, integration, and lack of centralized management
- **74%** want integration with cloud-native capabilities
- **93%** of those who have integrated DevOps and DevOps security into their operations report that they have faced security challenges when integrating security needs into those processes

These data points make it clear that multi-cloud poses a significant challenge for security professionals who must maintain traditional security policies with the tools available today.

The fact is, most organizations are relying heavily on their on-premises network security infrastructure when it comes to the cloud. In the 2018 MQ for Next Gen Firewalls, Gartner states that “as more organizations are moving strategic workloads to the public cloud, an increasing number seek to protect these workloads with their incumbent enterprise firewall vendor.”

> “83% have problems regarding next generation firewalls, including licensing, integration, and lack of centralized management.”
>
> – ***Dimensional Research Survey,*** *March 2018*

The problem is that a cloud and multi-cloud environment, existing appliance-based firewall vendors have legacy-oriented architectures that create significant scaling and management challenges for the cloud. Traditional network security infrastructure was built on an appliance model, initially hardware-based, and eventually, virtualized. This stands in stark contrast to cloud applications that are built using cloud-native principles. Appliance-based firewall vendors also base their cloud management model on a traditional on-premises based device manager model.

As an extreme example, some enterprises choose to back haul all cloud traffic to an on-premise location where they have appliance-based solutions installed, and then re-route application traffic to the cloud after traffic inspection and security enforcement. Enterprises do this because as Gartner states, “Today, these vendor offerings to AWS and Microsoft Azure are uneven. Some don’t offer the same level of inspection that on-premises firewalls do, and they all lack sufficient policy automation.”

The problems with appliance and device manager-centric approaches to network cloud security begin to point to what a modern, “cloud-native” solution should look like.

“As with agile development strategies, the allocation of security resources to inspect traffic or respond to a threat needs to be instantaneous. Unfortunately, many of the security tools available in cloud environments have not been fully optimized to take advantage of the functionality of the cloud, which can cause threat detection and response to be delayed or incomplete. In many respects, this is the same mistake that organizations made when they tried to extend their on-premise applications to the cloud.”

– CSO Online, April 2019

Requirements for Cloud-Native Network Security

Securing the cloud is fundamentally different than securing on-premise, physically located data center applications. A fundamental shift in the architecture of security needs to take place to address the cloud-natively – from the ground up—to get security moving at “cloud speed.”

Given the nature of cloud sprawl and dynamic application workloads, modern security solutions must meet the following requirements to be viable today:

- **Enable cloud app velocity, not inhibit it** – Application development and DevOps teams must be able to move fast to compete in today’s agile-driven world. Security ops cannot be an inhibitor and must adapt to the cloud rapidly and empower these teams. To achieve this, security must become automated and automatic like a pervasive fabric, able to react to workloads that appear and disappear rapidly.

- **Cloud visibility** – Traditionally, as enterprises have moved to the cloud, they have bemoaned the loss of control and visibility of the network infrastructure that runs their applications. With respect to network security, this requirement for increased visibility applies to both north-south and east-west (inter-VPC or inter-cloud) traffic. In addition, the modern cloud security solution must enable developers to use the cloud they want for their applications. By definition, a modern cloud security solution must be multi-cloud by design.

- **Management efficient** – Associated with moving at cloud speed, today’s network cloud security model remains complex, involving multiple layers of security where each of these are time-consuming to configure, manage, and at times, to scale. A cloud-native network security solution must take care not to increase the load of already overtaxed IT staff, and offer benefits of consolidation and reduced complexity.

- **App-centric** – Being application centric refers to a solution’s ability to be both management efficient and more efficacious in security. Being app-centric, a cloud-native security solution must be able to automatically discover, configure, monitor, and scale itself to applications as they come and go across one or more clouds. In addition, as application workloads move across VPC and cloud boundaries, being able to apply the right security protection and policies for that application leads to better security effectiveness by closing an otherwise open security hole.

- **Native cloud pricing** – Cloud-native security solutions should be structured for utility-based consumption. The appliance-based pricing of most traditional firewall vendors is an outdated remnant of ported on-premise appliances. Dimension Research found that 63% of security professionals preferred security delivered in a traditional cloud, pay-as-you-go pricing model than traditional appliance-based pricing. Appliance-based pricing requires guesswork to estimate purchases based on peak usage projections. These estimates often limit scalability down the road when projections come up short.

- **Cloud scale support** – With the cloud, services-designed applications benefit from the ability to enjoy elastic scale and unlimited throughput. Inline network security in particular must be able to support these high bandwidth requirements without introducing negative performance impact on latency.

A New Approach Needed

With these requirements in mind, it is safe to say that today's appliance-based solutions leave much to be desired. In addition, security offerings from cloud service providers such as Amazon, Azure and Google Cloud Platform, while cloud-native in some respects, are by definition not multi-cloud and nascent, making a consistent enterprise security strategy difficult.

Valtix is a new entrant into the cloud security market and has re-envisioned network security for the cloud. Below we map the requirements listed above for a built-for-the-cloud security solution to Valtix for a quick summary of our approach vis-à-vis existing network security offerings.

Requirement	Valtix	Traditional Appliance-Based Solutions
Enable cloud app velocity	• Valtix's platform is built on a global controller, enabling it to see apps in all cloud instances and adapt automatically as they come and go • Application discovery, configuration and scaling are handled automatically • Security is empowered to move as fast as application and DevOps teams	• Enterprises using virtualized appliance-based solutions lack global visibility • Requirement for cloud-specific scripting slows security ops down significantly and encourages DevOps to make convenient, less secure security choices
Cloud visibility	• The controller sits above all supported clouds and requires only credentials to see all applications	• Virtualized appliance solutions are not controller-based but device manager based, and lack the built-in visibility for multi-cloud network security
Management efficient	• The Valtix platform unifies TLS decryption, advanced firewalling, IPS, WAF and more in a single pass pipeline for unified security policy and enforcement at the FW • That same single pass approach enables built-in context for the information coming out of the platform – without external correlation engines • Easy deployment of Valtix cloud firewall clusters by centralized controller	• IT security teams must set-up and configure multiple products and enable scalability for each component • Administrators must move between multiple interfaces to study security threats vs one place
App-centric	• The Controller utilizes application tags to automatically enable application-specific security policy • Security policy moves with the apps	• Little capacity to apply specific security policy to the type of application or workload • Automatic discovery capabilities vary greatly
Native cloud pricing	• Priced as pay-as-you-go, utility-based pricing • Avoids scaling issues and guesswork on number of licenses to buy	• Priced as appliances, requiring guesswork to handle peak loads
Cloud scale support	• Intelligent built-in automated scaling from the Controller without boundaries • Valtix squeezes cloud infrastructure for performance – using advanced compute to increase throughput, enhance security, and reduce latency	• Bandwidth constrained based on appliances licensed • More expensive on massive scale out

About Valtix

Valtix is the industry's first, cloud-native network security platform for enterprises. Comprised of Valtix Cloud Controller and Valtix Cloud Firewall, the solution revolutionizes cloud network security with innovations that make visibility and enforcement automatic at the pace of the apps they protect. The centralized multi-cloud controller supports deployments for AWS and Azure (and GCP later this year). The firewall is architected with built-in auto scale, app-aware security policy and a single-pass pipeline for TLS, advanced FW, IPS, advanced WAF and more, which operates on a variety of cloud instance types from basic to the most advanced. For more information, contact us at sales@valtix.com or visit www.valtix.com.

VALTIX

Valtix, Inc.
2901 Tasman Drive, #222 • Santa Clara, CA 95054
650.420.6014 • sales@valtix.com
www.valtix.com