Valtix

Cloud Network Security Report 2019

Cloud Network Security Landscape, Challenges and Need for a New Architecture.

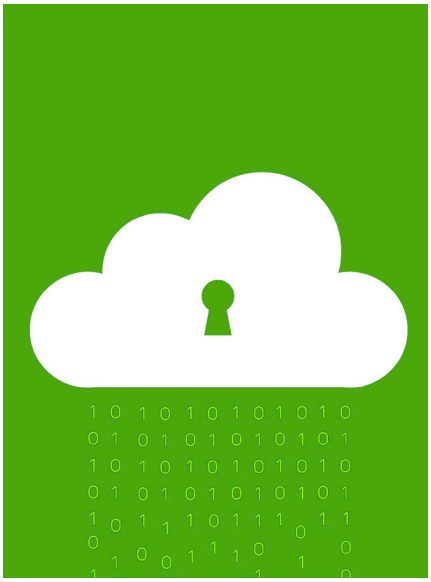
VALTIX

Security leaders are under a lot of pressure to show quick wins while knowing full well that everything they do will be heavily scrutinized and challenged, and ultimately, they will pay the price for things that are not under their control.” — **Yaron Levi, CISO, Blue Cross and Blue Shield of Kansas City**

Vatlix Cloud Network Security Report 2019

TABLE OF CONTENTS

01. The Cloud is the New Data Center



Just in case you weren't aware by now, the public cloud is becoming the new enterprise data center. In recent years, traditional enterprises have adopted to this concept rapidly by deploying a growing number of apps into the cloud — often in a distributed fashion. These organizations have taken advantage of the agility that is native to the cloud, placing applications that scale across dynamic networks in public cloud infrastructure. The security of those apps—built using an array of architectures such as IaaS, PaaS, public and private services—is still catching up, but network security, once again, is proving to be the common denominator.

Unfortunately, this new, dynamic environment has created new problems for organizations grappling with security in the cloud: keeping up with change, and providing a full suite of security services.

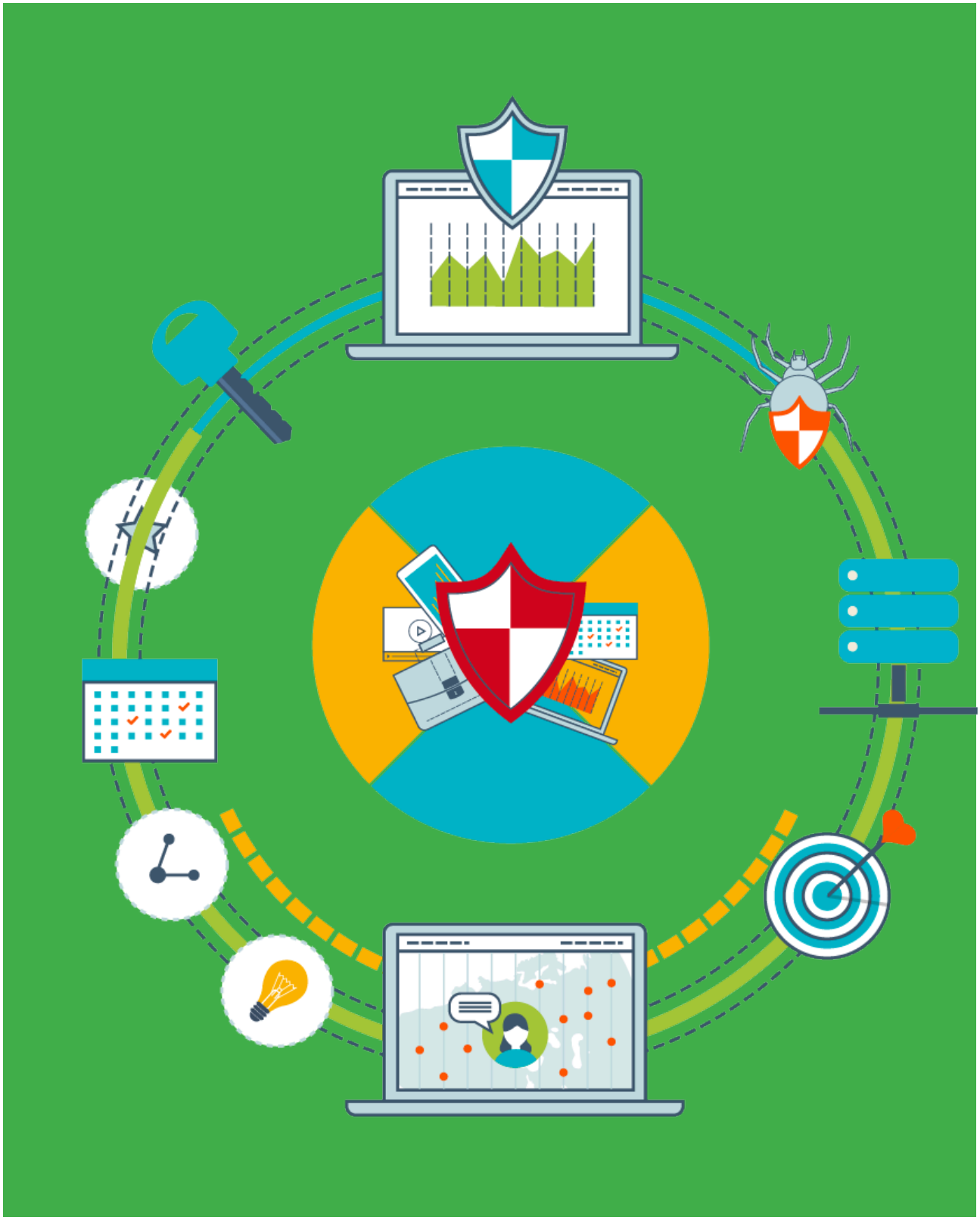
So, if apps are everywhere, placed by a variety of groups within the organization, and in constant motion along with their networks, the first problem is seeing and keeping up with that constant change. Not "automation" in the traditional sense (simple scripting of predetermined actions and responses), but technically an "automatic" capability — where changes do not have to be foreseen.

The second problem is really the (in)ability to provide a complete and consolidated set of enterprise network security services in this environment, such as TLS, firewall, IPS, and WAF.

VALTIX

“On average, companies with fewer than 1,000 employees run an average of 22 custom applications. The largest enterprises with more than 50,000 employees run 788, on average.

More Apps are being built in and for the Cloud. Over 75% of Public Cloud IaaS Budget Spending are allotted for Engineering, Operations, and Development...”



02. Cloud Network Security Mis-steps

When experimenting with apps in the public cloud, many organizations simply backhaul traffic to use existing network security infrastructure. The problem is that many of the existing tool sets—such as public cloud provided tools and traditional enterprise network security tools—can't provide effective help.

To their credit, public cloud-provided tools are cloud native, dynamic, and scale easily. The downside is that they lack policy depth and breadth, and are single-cloud only. Public cloud-provided tools are really only designed as a checkbox — where enterprises can hear the answer, "yeah, we have a firewall," and simply check the box to move apps to the cloud.

Traditional enterprise network security tools were initially designed for the on-premises datacenter, and have rich services and strong policy. Unfortunately, they are virtual appliances built for a static environment. Being a port from hardware appliances, they are unmoored from the hardware acceleration they were designed for, resulting in poor performance.

Many organizations turn to next-gen firewalls (NGFWs) as the modern answer to network security. Unlike traditional firewalls that track the domains where traffic is coming from, and the ports it's traveling to, next-gen firewalls also monitor the actual content of the traffic for any malware and data exfiltration, and then react accordingly.

Legacy boxes are not built for the cloud. While better than traditional firewalls, NGFWs are still premises-based, and can no longer provide protection when users move beyond the perimeter network, or use mobile devices and apps that transmit data in the cloud.

However, organizations don't have endless security assembly line to meet up the new dynamic speed demand with current silos and fatigue.

The bottom line here is that security needs to follows the apps in the cloud.

03. Lessons from Cloud Network Security Breaches & Incidents

Reference: Top 5 Network Security Breaches

Capital One

On July 29, 2019, FBI agents arrested a woman on suspicion of downloading nearly 30 GB of Capital One credit application data from a rented cloud data server, affecting 100 million people in the United States and six million in Canada. That data included nearly 140,000 Social Security numbers, 80,000 bank account numbers of U.S. consumers, and close to 1 million Social Insurance Numbers (SINs) for Canadian credit card customers.

How it Happened:

The breach stemmed in part from a misconfigured open-source Web Application Firewall (WAF) that Capital One was using as part of its operations hosted in the cloud with Amazon Web Services (AWS). The misconfiguration allowed the suspect to trick the firewall into relaying requests to a key back-end resource on the Amazon Web Service platform that Capital One used to host much of its data.

Equifax

Equifax, one of the major credit reporting companies that calculates credit scores for financial institutions and insurance companies, reported a massive security breach on September 7, 2017. The company reportedly lost control of customer data that included the Social Security numbers, birth dates, and home addresses of 145.5 million US citizens, including a number of driver's license numbers, credit card numbers and dispute documents.

How it Happened:

The incident was caused by a misconfigured Amazon Web Services (AWS) S3 Bucket that exposed the 36GB worth of data to the public. The data consists of 248 categories, including specific information such mortgage and consumer demographics in addition to addresses and contact details.

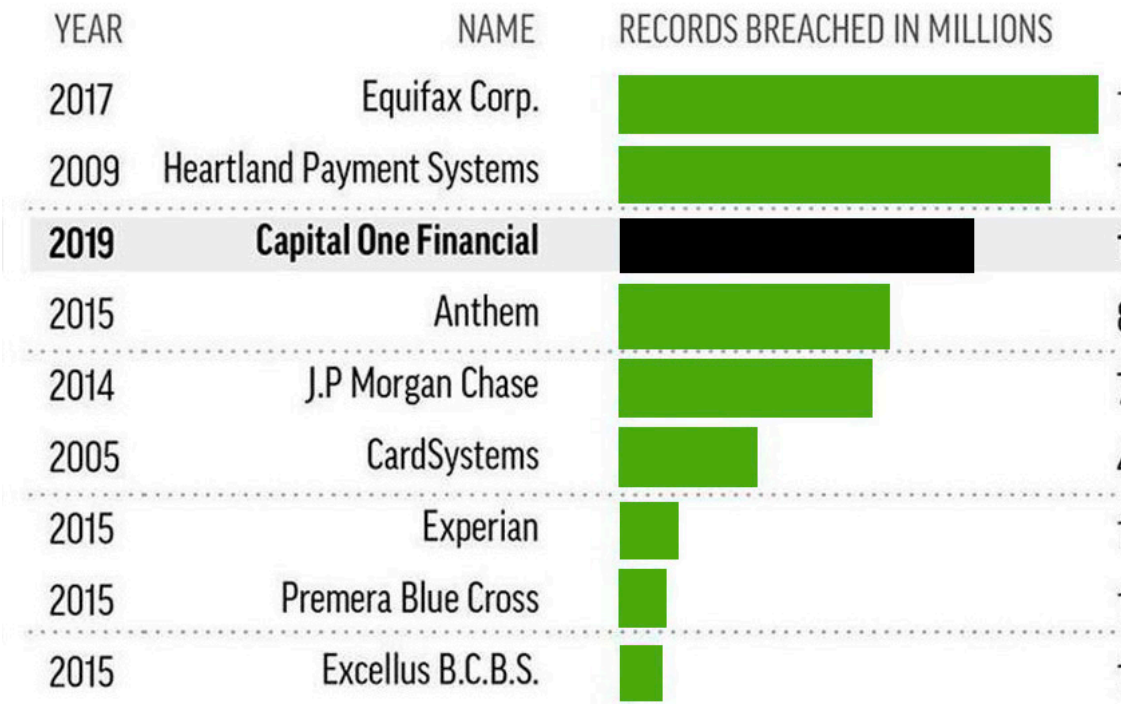
Yahoo!

Yahoo has actually been the subject of multiple breaches, including 2013, 2014, and the discovery of a massive breach in 2016 that had been ongoing for several years. The breach resulted in the access to data of all 3 billion users, and the full fallout of the three incidents is still not yet known.

How it Happened:

Experts are still having Yahoo has actually been the subject of multiple breaches, including 2013, 2014, and the discovery of a massive breach in 2016 that had been ongoing for several years. The breach resulted in the access to data of all 3 billion users, and the full fallout of the three incidents is still not yet known.

Top 10 Industries Where Data Breaches are Most Expensive



Source: Splunk 2019

Lesson Learned: Valtix Answers

Valtix Blog: Network Security for PaaS Workload

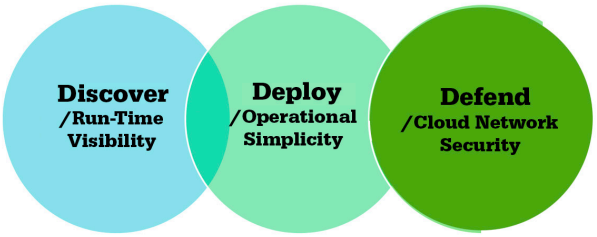
Many AWS related security incidents are involved with WAF misconfiguration and policy enforcement with S3 access. A Valtix's blog highlights the root causes and how you can jointly resolve & prevent further breaches in Public Cloud.

Deploy Valtix' Discovery solution that builds an evergreen model of your apps and infrastructure. Tag your applications and create the corresponding policy.

1. Valtix will ensure that the policies move with your apps as the footprint changes or increases across your public cloud deployments.

2. Use Valtix's WAF solution to protect the Application. Build WAF profiles to protect against SSRF attacks. These profiles can be used in all of your multi-cloud deployments. You can also extend from a Valtix provided cloud friendly WAF profile that has this policy enabled by default.

3. Implement micro-segmentation using tag-based Address Objects to enforce fine grained access to S3 within the AWS infrastructure.



4. Implement full DPI of S3 services. This is optional. This requires changes in the applications accessing S3 to go via proxy. Access S3 by an internal Valtix' powered proxy endpoint. Enable rich IPS policies to defend against exfiltration of data based on configured regular expressions. This step would have prevented the attacker who assumed the IAM credentials of the app server from downloading the consumer application data from S3.

04. Are AWS, Azure and Google Cloud Secure?

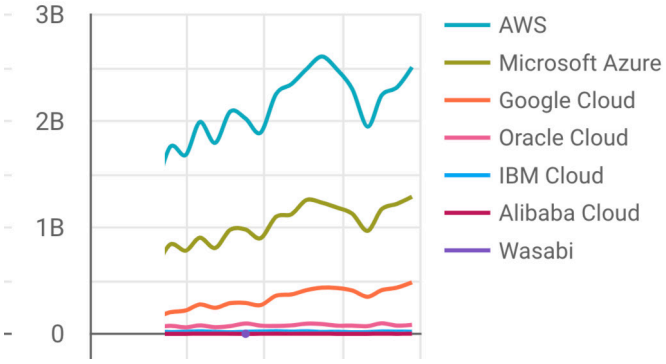
Google, Microsoft Azure, and Amazon continue to be the most popular cloud-hosting services in the world, utilizing their extensive resources in order to create cloud networks capable of supporting some of the world's largest entities — along with general consumer usage as well.

In fact, global spending on public cloud computing is expected to increase from $67B in 2015 to **$162B by 2020** (Source: Forbes) — 6 times the rate of predicted IT spending. Even so, cybersecurity defenses have not kept pace with public cloud adoption, which continues to create glaring security holes and liabilities.

The truth is that cloud security is a shared responsibility between the cloud service provider and the organization itself.

Cloud service providers like Amazon, Google, and Microsoft are responsible for managing the security of their clouds, and seem to be doing their part currently, avoiding responsibility for any major breaches thus far.

On the other hand, organizations are responsible for monitoring their own network infrastructures for liabilities, nefarious user activities, hostile network traffic, and host vulnerabilities. The inherent security of cloud service providers towards their own respective clouds does not account for this; it is up to the organization to equip itself with effective security for its data in motion and data at rest — whether that's within the confines of its own perimeter, or for devices and users outside of it.



IaaS account activities increase by 45% with data collected from Jan 1, 2019 - June 1, 2019 by Budgets Research.

05. Why Use Cloud Native Network Security?

Traditional network security appliances cannot scale or keep up with the apps they are supposed to protect.

Today's organizations require elasticity, high availability, and resilience. Native security services in IaaS (such as AWS/Azure/GCP) with a Shared Responsibility model only provide basic "checkbox" functions with insufficient policy depth and breadth.

Existing security approaches force organizations to choose between less security (due to the inability of appliances to adapt to highly agile applications,) or less agility, as virtual appliance-based security restrains growth and mobility of cloud apps

Using an excessive multi-vendor approach depletes security management and DevOps resources while hindering consistency across platforms

True MultiCloud Support

See and control across your VPCs, regions and accounts, automatically discover apps and enforce app-specific sec policies

Predictable Deep Inspection Perf

Experience better performance, efficiency and effectiveness with patented data plane

Consolidated Advanced Sec Service Chain

Use a single policy and data plane for TLS, advanced firewalling, IPS, WAF and more; benefit

Native Elastic Workload

Leave scripting and administrative work behind, our controller handles auto scaling for you

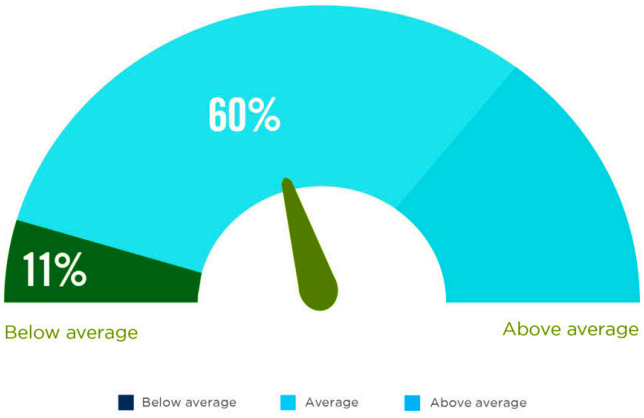
Pay As You Go

Consume your security the way you consume your cloud, with utility-based pricing

Context Rich Insight

See violated rules and potential attacks across L4-L7 and APIs in one place without external correlation

06. Current Cloud Challenges for Enterprises



> The top cloud security concern of cyber security professionals is data loss and leakage (64 percent). Only 29% of Security Readiness respondents thinks their security is above average."

- Extending on-premises data centers to the public cloud (e.g., AWS, Azure, GCP). Deliver security consistency over cloud apps with microservices and APIs.
- Serverless application needs serverless security. Full life cycle network security (management, scaling, network and availability) is required over across varied classes of applications such as serverless functions, PaaS, Container clusters, Scale-out virtual instances etc.
- Lack of automatic network security deployment. Apps are dynamic and elastic, networks are dynamic and elastic, but network security is static. Need Cloud subject matter experts
- Automating network security by implementing "Network as code" support with terraform resources etc.
- Advanced security beyond native security services in the Public Cloud
- Deploy a full stack of security services autonomously as business-critical apps grow
- Full-scale end-to-end encryption
- Vendor lock-in is also concern for those moving to the cloud. You can mitigate the risks by selecting a Pay-As-You-Go subscription structure. Cloud lock-in can be avoided by selecting your multi-cloud network security solution

07. Cloud Network Security Check-list

Effective cloud network security can be broken down into three core aspects to check off: Discover, Deploy, and Defend.

Discover.

Discover - this is not a point-in-time process, but an ongoing modeling of the environment to not only see which apps are where and how they are changing, but enable action.

- Show me all of my apps across clouds, regions, VPCs/VNets
- Keep inventory up-to-date as apps and networks change
- Provide a map for me to overlay security infrastructure and policy onto

Deploy.

Deploy - This is a continuous action in a dynamic environment. Not only do enterprises need to deploy netsec once, but continuously in the cloud — where apps and networks are changing.

- Deploy network security infrastructure onto the model (from Discover)
- Scale infrastructure up/down as needed
- Ensure that the correct policy follows the app wherever it goes

Defend.

This is a continuous process, where organizations need to:

- Provide the correct suite of netsec services
- Implemented in an integrated way, where single data path, single policy, single telemetry feeds result in predictable performance and efficient ops
- Implement in an integrated way, without gaps

08. How Valtix Meets Cloud Security Needs

Discover, Deploy, Defend is the process template around which Valtix built its network security platform. Siloed, legacy tools with complex stitching using scripts and Lambda functions simply cannot fulfil these requirements.

In order to implement an effective approach, we built two components:

- **Valtix Cloud Controller**: SaaS-delivered, multi-cloud, normalizes policy across clouds, provides an evergreen model of the environment, and deploys the data plane.
- **Valtix Cloud Firewall:** Cloud-specific to take advantage of each cloud environment, multi-service gateway, automatically scales, and provides follow-the-app security.

Valtix revolutionizes inline cloud network security, with innovations that make visibility and enforcement automatic at the pace of the apps they protect:

- **Cloud-Native** – Possesses all of the attributes of a cloud-native capability: automated app discovery and elastic scaling, multi-cloud support and automatic

adaption.

- **Unified** – Consolidated security across TLS, advanced firewall, IPS, WAF and more, with a single policy that follows the application
- **High Performance** – Not just high throughput and low latency, but rapid and automatic response to application deployment, change, and growth

Valtix is more innovative than existing products because

- Platform-native, full (on-going) application and network discovery; cloud-native deployment capabilities (auto-scale, tag-based policy, edge to transit gateway deploys); and, rich security services for best-in-class defense.
- Highest-performing (**bandwidth +50Gbps**, **latency <8ms**) security services with an industry's first, single-pass pipeline of forwarding and proxy services: TLS, Advanced Firewall, IPS, WAF and more.
- Fast deployment (order of seconds to minutes) and real-time reaction (order of seconds) to application inventory changes
- Supports most network and application resiliency **up to 5 Availability Zone** deployments.

09. Valtix Use Cases

Key use cases including edge security, hub & spoke topology and accelerated high performance compute...

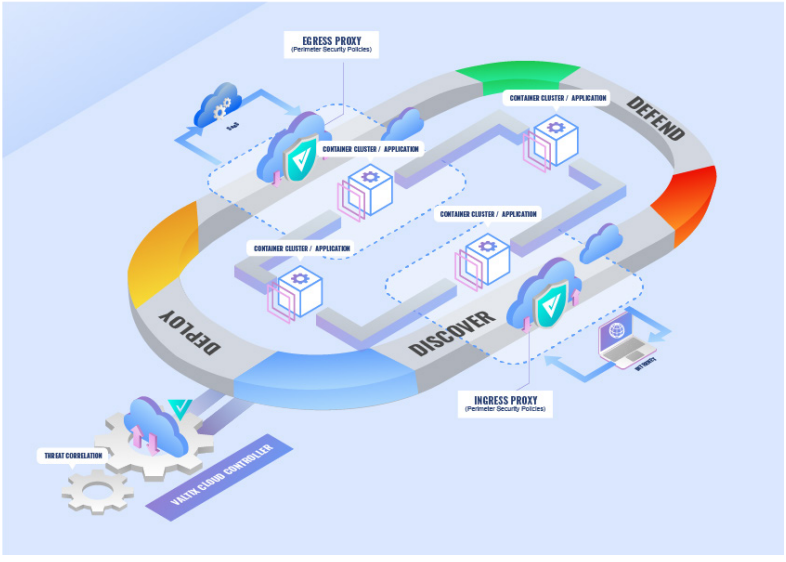
1. Ingress and Egress Cloud Edge Security Control

- Valtix protects against app traffic entering into the boundary of the Cloud. Egress means traffic leaves from inside the private network out to the external SaaS or public internet.

- Instead of “rack-n-stack”ing excessive virtual instance footprints for high availability and mixing with native NLB/ELB/ALB or trying to build the scalability by scripting, Valtix Security Platform brings “single-click” Ops with secure controls with auto-provisioning and cloud-native elasticity at the Ingress and Egress points without the need for additional correlation.

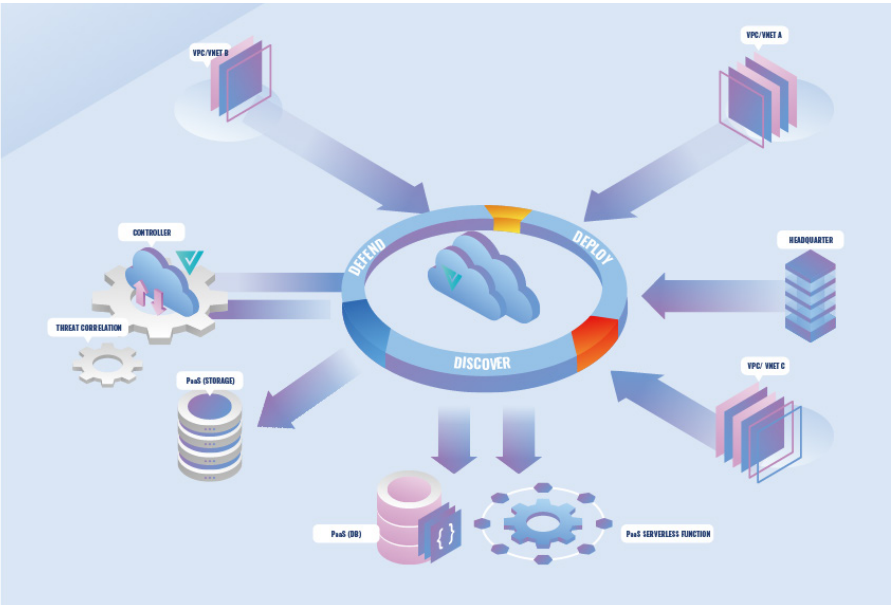
- Traditional bolt-on NGFW at the cloud edge typically increases latency and introduces scale challenges. As security follows cloud apps deployed as services and APIs, predictable latency is must-have checkbox through single-pass security architecture and advanced compute instance.

- Encryption everywhere means zero air gaps from Ingress entry to Egress exit. Valtix brings end to end TLS for built-in rich security services.



2. Hub and Spoke with AWS Transit Gateway

- This use case eliminates network security management complexity when enforcing security policy dynamically across cloud regions and VPC/VNets
- Scales with Apps – Supports tag-based policies for East-West bound and continuous discovery through intuitive workflow-based dashboard
- Scales with Traffic - Elastic, scale up or scale out
- High Availability - No AZ limit, decoupled control plane and data plane



10. Valtix Advantage

Enterprises are at various stages of cloud adoption. All need an approach to network security that thrives in the Cloud – and moves at cloud speed. Existing security appliances can't scale and adapt as fast as your app.

The Valtix team has built products in security, infrastructure and cloud, which are currently deployed in tens of thousands of enterprises and resulting in billions in annual revenue.

Download Valtix Data Sheet

Download Valtix Guide to Cloud-Native Security

Our free cloud native security guide covers:

- Why the data center is now amorphous and likely to cause sprawl issues in your environment
- How applications have changed over time, and the impact that's had on security
- Why security teams are regarded as slow in the DevOps era — and what to do about it

Schedule a demo with Valtix Security Expert Today.

Contact Information

Valtix, Inc.

www.valtix.com

2350 Mission College Blvd, #800
Santa Clara, CA 95054

650.420.6014

According to the State of Application Delivery survey, app developers care about speed, scale and security. The research found that they prioritised app acceleration (34%), Web Application Firewalling (WAF) (26%), load balancing (21%), Transmission Control Protocol (TCP) optimisation (20%) and content caching (17%) among other application services.

Valtix, Inc.
2350 Mission College Blvd, #800
Santa Clara, CA 95054
650.420.6014
www.valtix.com