VALTIX

THE CLOUD ARCHITECT'S GUIDE TO NETWORK SECURITY

How to design a security architecture that meets the cloud's unique requirements

In the last few years, the momentum behind "shift-left" has resulted in the development of more secure applications, with software developers adding security earlier in the development lifecycle. While protecting applications inherently through "shift-left" has been a positive change for DevOps, the recent Log4J/Log4Shell events demonstrated that software vulnerabilities will always be present.

Log4J is proof that to protect your applications, you can't rely solely on the controls within those apps. So what does it mean for your cloud architecture when simply writing secure apps and patching is not enough?

Whether you have a vulnerability for only a few short hours or for entire months, threat actors will take advantage of any window of opportunity to exploit it. You need to add defense layers outside of the app, making network security as relevant in the cloud as it is on premises. The challenge is that traditional security models (such as virtual appliances or hardware appliances in the data center) fall short of the cloud's requirements. And while each cloud provider has its own stack of network security controls, they are often incomplete, expensive, and not integrated. They also don't meet the multi-cloud requirements of most organizations and instead create an unsustainable single cloud solution.

While many of the traditional network controls are still critical in the cloud, those controls must adapt to the unique cloud environment. This ebook will help cloud architects understand how to design security models for cloud-native workloads and applications.

How network security is different in the cloud

The cloud is dynamic rather than static, with ephemeral workloads, changing network addresses, elasticity, automation, and seamless scalability. Your cloud security architecture must adapt to this ecosystem — providing automated protection while learning and adapting to the environment.

Taking a Comprehensive Approach to Cloud Security

In the past, the purpose of network security was to secure the network itself, and applications simply inherited that security. But, as recent events have demonstrated, you need to approach cloud architecture differently — and protect the applications regardless of the underlying infrastructure. That's where network-based controls come in to provide the additional layer of security for your cloud workloads. This is also required for meeting common compliance and regulatory frameworks such as ISO, SOC, and PCI DSS.

A comprehensive approach to cloud security requires defense in depth, along with a combination of passive and active defenses. But to keep up with the cloud's dynamic environment, the controls must be automated while constantly learning from, and adapting to, the environment.

Six Critical Components of Cloud Security

Visibility into assets, traffic, and activity — providing visibility into both security posture (e.g., exposed workloads, open network paths, vulnerabilities) and network activities (e.g., exfiltration, lateral movements and attacks, communication patterns)

Elastic scale — scaling security capabilities automatically along with the cloud workloads they're protecting, without the need for complex logic of different parameters and thresholds. Security should scale the same way compute, networking, and storage scales.

Self-healing security infrastructure — automatically identifying failures and autonomously remediating them to quickly solve problems when vulnerabilities are found or something breaks down in the cloud security infrastructure

Infrastructure-as-code (IaC) — eliminating manual processes and automatically integrating security into the deployment cycle (e.g., into tools like Terraform)

Identity and context (workload and user) — integrating dynamic asset discovery and tagging in near-real time to automatically identify and contextualize information for cloud assets (eliminating ineffective, broad security policies)

Multi-cloud support — eliminating the complexities of separately managing each cloud's security, as well as reducing the cost to train for each provider's security architecture

Architectural Considerations for Cloud Security

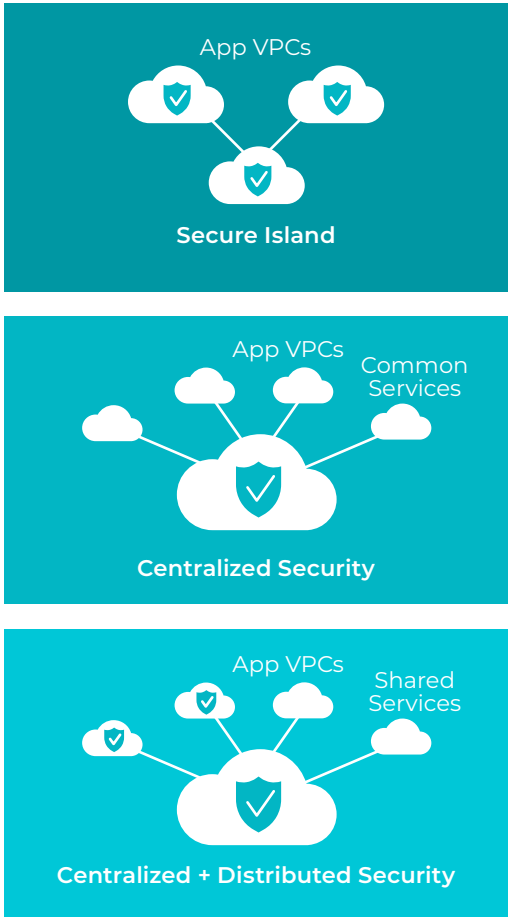
There's no "one size fits all" model for architecting cloud security. To implement a control point between cloud workloads and the public internet, you can use a centralized, distributed, or hybrid model.

Although the idea of centralized control and enforcement sounds good in principle, it's not always the best approach. For example, centralized control with distributed (or local) enforcement may work better in many cases because it avoids sending traffic across trust boundaries to secure it. Some applications may also require more isolation for compliance reasons. That's why it's important to understand the benefits and drawbacks of each approach before choosing the best combination for your environment.

- **Centralized control:** provides global definition and management of policy across large multi-cloud deployments. This model enables you to define consistent policies regardless of where the application is located; it also provides visibility for all types of security events. Avoid single point of failure of legacy architectures by implementing centralized controls with cloud-native design patterns — including multi-availability-zone (AZ) and multi-region architecture, along with elastic cloud-native services.
- **Distributed control:** spans across different security appliances that must be integrated to work together. This enables more granular security controls, but it also lowers your visibility across multiple clouds and creates redundancies or inconsistencies. Management and support costs also go up in this model.
- **Centralized enforcement:** requires routing all traffic to a central point, which provides consistent policy enforcement, but also introduces compliance issues and creates inefficiencies.
- **Distributed enforcement:** keeps traffic close to the application for local enforcement, enabling you to define policies for specific application requirements and enforce policies quickly and reliably, but can be difficult to operationalize at scale.

A mixture of both distributed and centralized enforcement can provide a suitable blend with web security provided in a distributed model and security for other aspects of the app provided in a more centralized model.

Cloud Security Architecture



The Shortcomings of Existing Approaches

Virtual Security Appliances

Many organizations lean toward extending their data center appliances into the cloud (e.g., Palo Alto Networks VM-Series, Checkpoint, Fortinet, etc). This model doesn't work well because of the appliances' inherent inability to work well in a dynamic cloud environment. The disadvantages include:

- Lack of native autoscaling, creating operational complexity due to unsupported scripts and resulting in excessive costs to correctly customize and maintain
- Lack of integration into cloud networking constructs such as AWS transit gateways, making it hard to scale security to tens and hundreds of VPCs, and breaking the cloud network architectures
- Lack of cloud-native workload identity, resulting in poor security coverage due to manual association of application IDs with cloud workloads
- Lack of cloud scale, resulting in reduced agility due to manual management
- Lack of a single dashboard for centralized policy enforcement, along with fragmented visibility across multiple clouds

IP-Based Network Security Policy

In the data center, you can set network security policies based on IP addresses to govern the behavior of network devices and users. Since IP-based policies are relatively static, they don't scale to the cloud, where IP addresses change dynamically — for example, when an instance is shut down or when autoscaling occurs.

Security Groups

Security groups provide basic security segmentation and help reduce your attack surface by restricting network port access. But they give you a false sense of security. Cloud applications require certain network ports to be accessible in order to function, and security groups cannot stop attacks that target these open ports. Security groups also offer limited visibility due to the lack of logging and contextual metadata needed when responding to incidents. Additionally, since they only allow you to create a small set of rules, security groups don't scale well across dozens of applications.

88% of IT leaders say that bringing network security appliances to the cloud is challenging to the cloud computing operating model.[1]

[1] "How Log4SHELL Changed Cloud Security," Valtix, 2022

Requirements for Protecting Cloud Workloads

Layered defenses must consider capabilities such as visibility into all your assets, protection against web-borne threats, and cloud network security. Next, we take a look at key considerations such as network segments, use cases, and critical capabilities your security solutions need.

Traffic Paths (Network Segments)

To stop malicious activity across your cloud infrastructure, applications, and services, you need to secure both the perimeter (ingress and egress, or north-south traffic) and lateral traffic (east-west).

Ingress: covers traffic initiated by another location to your cloud workloads. Examples include general public access to a website or application, and partner access to an API gateway. The direction is inbound and client-initiated. Securing ingress protects your cloud applications from internet-facing attacks and unauthorized external access; it also prevents further lateral movement to the rest of your cloud deployment.

Egress: covers workloads initiating traffic to somewhere else, or what your cloud deployment needs to access to perform an operation or function. Examples of access include external payment gateways, API-based services, SaaS services, software updates, and external URLs. The direction is outbound and initiated on the application side. Securing egress protects applications from threats such as malware (by preventing command-and-control or C2 action) and data exfiltration.

East-west: covers workload-to-workload traffic within the cloud environment or on premises (hybrid). Examples include communications such as inter-region, endpoint services, private links, or PaaS constructs. These can be either client- or server-initiated. Securing east-west traffic prevents lateral movements of threats within your cloud deployment.

Typical Network Security Controls

NETWORK SECURITY FUNCTION	INGRESS	EGRESS	EAST-WEST
Web Application Firewall (WAF)	✓	–	**
Intrusion Detection/ Prevention (IDS/IPS)	✓	✓	✓
Segmentation (Firewall)	–	–	✓
AntiVirus Detection/ Blocking	✓	✓	**
URL/FQDN Filtering (includes Explicit and Category based profiles)	–	✓	✓
Data Loss Prevention (DLP)	–	✓	✓
Layer7 DoS	✓	–	✓
Malicious IP Blocking	✓	✓	–
GeoIP Blocking	✓	–	**
Threat Packet Captures	✓	✓	✓

** Optional, dependent on architecture.

Key Security Use Cases

Web application security:

Basic web application attacks are the second most-common pattern involved in both data breaches and security incidents, according to Verizon's Data Breach Investigation Report. As mentioned earlier, there's increased pressure to secure applications not only within themselves but also at the network level. This is where web application security — such as a web application firewall (WAF) — comes in, protecting your cloud apps from intrusions and vulnerability exploits from outside the workload.

Microsegmentation/zero trust:

Connectivity between workloads is ubiquitous in the public cloud, which can allow a direct path to the internet. Implementing a zero trust model is one way to solve this issue. Quickly becoming the standard approach to security, zero trust is effective in the cloud because it assumes that no entity or connection is secure, even if it's located within the network.

Microsegmentation enables you to implement zero trust in the cloud by defining granular policies to enforce least privilege access between (east-west) and to or from workloads (north-south). The challenge is that many organizations implement microsegmentation using the same agent-based solution they have in the data center, which creates operational challenges and dependence on the underlying workload infrastructure. This impacts security by fragmenting visibility and creating gaps. In addition to microsegmentation-based access control, you can also layer in traffic inspection to prevent lateral movement of threats.

Egress security:

Since most workloads require third-party services, having visibility and control over outbound connectivity is essential. Egress security blocks unauthorized external communication to protect your workloads from threats such as malware distribution, unsecure APIs, and sensitive data exfiltration. Egress security requires TLS decryption for content inspection, URL/FQDN filtering, data loss prevention (DLP), and malware detection.

Core Capabilities for Your Cloud Security

Network access control (firewall): provides control over connectivity between workloads via policy. Essential for least privilege access, zero-trust microsegmentation, and adherence to compliance mandates. Cloud-native constructs such as content security policy (CSP) tags are critical to creating policy definitions that are resilient and adaptable to frequent changes.

Web application protection (WAF): detects and blocks malicious traffic, based on rules, to protect applications and APIs against external threats including denial of service (DoS) attacks and malicious IPs; can also restrict access based on user/IP geolocation.

Threat prevention and detection (IDS/IPS): provides real-time protection against network attacks, exploits, and exposures in application code and operating systems that workloads run on; instrumental in virtual patching against exploits of vulnerabilities such as Log4Shell.

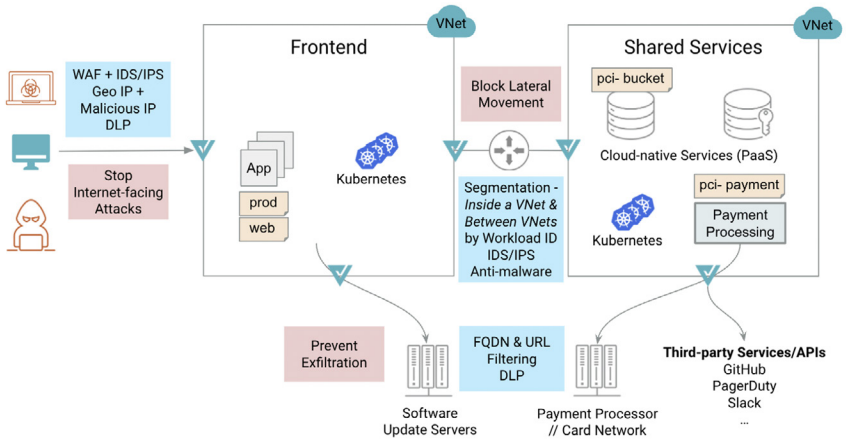
Exfiltration monitoring (DLP): provides visibility and control into the movement of sensitive data in your cloud environment; enables you to set content- and context-based policies based on the thresholds of monitoring, alerting, and potentially blocking of unauthorized activity.

Outbound connectivity control (egress filtering): controls outbound destinations from cloud workloads, using URL and FQDN filtering (custom lists and category-based) to prevent unauthorized connections (such as C2 communication) and data exfiltration from cloud applications.

Malware detection and prevention (AV): detects and blocks threats such as viruses, trojans, and ransomware based on signatures without the need for host-based agents.

Network traffic decryption (TLS decryption): a foundational capability that enables security outside of the app workload to provide complete visibility and protect against hidden threats. Cloud decryption requires high throughput performance and low overhead that can't be provided by virtual appliance offerings.

Comprehensive Multi-Cloud Workload Protection



Recommendations for Implementing Cloud Network Security

Organizations typically consider three options for implementing cloud network security:

- Deploying virtual appliances previously used on premises
- Relying on the cloud provider's security stack
- Using third-party cloud-native tools or platforms

As discussed previously, extending virtual appliances to the cloud is not an ideal option because these legacy solutions are not designed to work in the cloud's fast-changing environment.

Cloud network security services offered by cloud providers are often too complicated to integrate between functions, which increases deployment costs. Additionally, these controls typically don't go deep enough to provide adequate protection. And since they vary from one provider to the next, your security will be inconsistent across different clouds and leave gaps.

Cloud-native security solutions work best for cloud environments because they inherit the characteristics of the cloud to meet the cloud's requirements. Consequently, cloud-native platforms:

- Offer agility, scalability, and elasticity
- Enable continuous asset discovery and automated policy enforcement
- Work seamlessly with your apps and deliver consistency across clouds

One differentiation among cloud-native solutions is whether they rely on agents or not. Solutions that use agents are more complicated to deploy and manage, which could result in rollout and maintenance delays, as well as increased operational overhead.

The Importance of Automation in the Cloud

Automation is one of the important benefits of cloud-native security solutions. In the cloud, everything constantly changes and evolves, and security needs to learn and adapt quickly to these variations. Automated controls minimize the risk of manual errors, reduce overhead, and enable your security to move as fast as your application teams and business agility requirements. But not all automation is created equal — natively automated processes decrease deployment and maintenance efforts, whereas add-on automation (such as scripts) increases those efforts by adding more things you need to deploy and maintain.

Why Cloud Network Security Platforms Are the Future of Cloud Security

While the cloud requires a defense-in-depth strategy, implementing individual controls through point solutions creates fragmented visibility, duplication, and coverage gaps. Cloud security platforms solve these challenges by strategically consolidating visibility and control into a single, integrated system.

A cloud network security platform (CNSP) provides a comprehensive approach to multi-cloud network security, allowing you to consolidate visibility and efficiently secure with unified policy. This approach reduces your mean time to detect (MTTD) and mean time to respond (MTTR), cuts costs, and boosts your cloud security posture.

A purpose-built CNSP combines multiple capabilities, providing:

- **Continuous visibility** into your network posture, including real-time asset discovery and inventory, assessment of open network paths, and suspicious traffic detection
- **Cloud workload protection,** securing ingress, egress, and east-west traffic so you can detect and block malicious or prohibited activity, prevent lateral movement, and meet compliance requirements
- **Web protection** for your applications and APIs through a single-policy framework

The advantages of a cloud-native platform include:

Single policy management — eliminating overlapping controls at various defense points, saving you time, reducing complexity, and enabling more consistent security that reduces the attack surface.
Business impact: risk reduction

Overall improved effectiveness — reducing overhead, minimizing manual errors, and improving MTTD/MTTR by automating a variety of processes.
Business impact: cost and resource efficiency

Lower latency and higher performance — decrypting traffic once for all your security controls through single-pass inspection so you can improve the user experience without compromising protections such as resource-intensive east-west traffic decryption.
Business impact: business resilience and agility

The best cloud-based security platforms scale on demand when you need additional capacity and integrate with open-source automation solutions and other third-party tools such as SIEM, SOAR, and threat intelligence. These security platforms enable you to simplify business processes and user training, reduce implementation and maintenance costs, and lower your overall security and business risks.

Future-Proof Your Cloud Security Architecture

Your cloud network security needs to be flexible so it can accommodate both your current needs and future state. As you develop your cloud security architecture, consider how quickly and seamlessly it will be able to adapt to the evolution of your cloud environment.

The cloud offers speed and agility so you can transform your business and remain competitive. But you can't deliver on this promise if your cloud security doesn't keep up. Choose a cloud security model that helps you accelerate your cloud initiatives rather than becoming a hurdle.

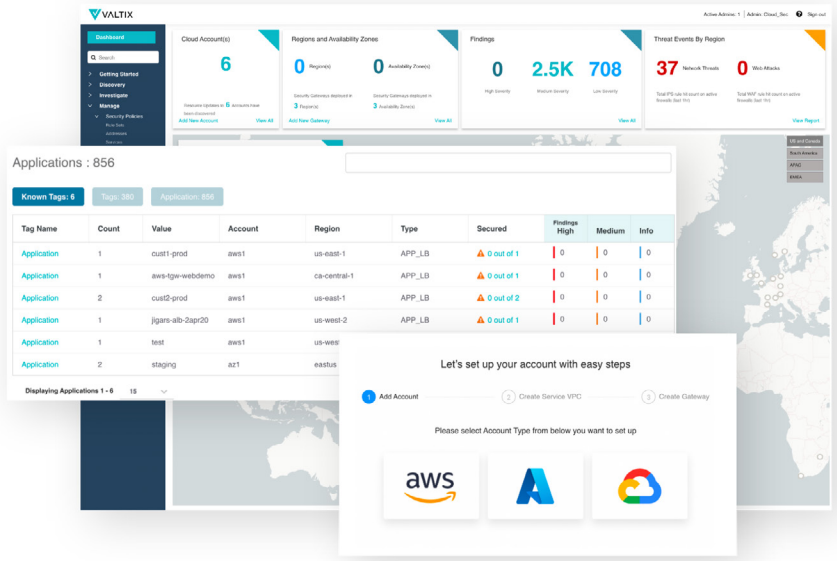
Implement Multi-Cloud Security in 5 Minutes with Valtix

Valtix offers a cloud-native, purpose-built, cloud network security platform that consolidates multiple security capabilities to deliver an end-to-end, integrated approach to protecting your cloud workloads and applications with a single multi-cloud policy. The agentless, appliance-free platform scales on demand and integrates out of the box with tools such as Terraform, ServiceNow, and Splunk.

With Valtix, you gain:

- Fast, 1-click deployment via a SaaS console
- Proactive, layered, advanced security controls
- Security policy automation based on context through tags
- Reduced maintenance with no scripts
- 10X productivity boost due to consolidated workflows and minimal upkeep

Robust, advanced cloud security doesn't have to be complicated. Valtix cuts your operating expenses, reduces your time to market, and lowers your risk — so your business can move as fast as the cloud without making compromises.



Request Demo Sign Up Free

About Valtix

Valtix is on a mission to protect every workload, every app architecture, across every cloud. The first multi-cloud network security platform delivered as a service, Valtix was built to combine robust security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture, Valtix provides an innovative approach to multi-cloud security that is deployable in just 5 minutes and adapts to changes in seconds. The result: security that is more effective 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.

Join 4 of the top 10 pharmaceuticals and leaders across every industry and sign up free in minutes.

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