WHITE PAPER

VALTIX

ACHIEVE ROBUST CLOUD SECURITY WHILE MAINTAINING AGILITY

Requirements and considerations for protecting cloud workloads through network security while enabling the acceleration of business initiatives

The Cloud Is Dynamic. Security Must Adapt.

In a changing world where digital transformation equals business resilience, no one would argue that a cloud strategy plays a pivotal role. But, as a result of the recent Log4J incident, organizations' enthusiasm to implement their cloud roadmap may have waned.

A recent survey of cloud security leaders by Valtix found that Log4J/Log4SHELL was a wake-up call — 95% said the incident would change cloud security permanently.[1] This adds to the hesitation that many organizations already had about their cloud initiatives.

Staff shortages, lack of skills, and fractured visibility are among the many factors contributing to poor confidence in cloud security. But ultimately, the main reason organizations struggle is because they view their cloud environment as an extension of the data center. Consequently, they adopt the same old-school security design as they do on premises.

Securing the cloud entails some of the same tools that are effective for perimeter security. But the similarities end there. The cloud has unique requirements — and without meeting those requirements, your security will remain inadequate.

Some of the primary differences in the cloud include:

- Dynamic rather than static nature
- On-demand elasticity
- Seamless scalability
- Speed to deployment and business agility
- Lack of control over cloud services (serverless/PaaS)

While **89%** of IT leaders believe cloud security is different, **75%** see the cloud as an extension of the data center.[2]

85% of IT leaders agree that it's more challenging to secure workloads in the public cloud than in an on-premises data center.[1]

44% of organizations aren't sure that their cloud workloads are secured to the same degree as their data center.[1]

Everything in the cloud is constantly changing and adapting to new conditions. Assets are highly interconnected, processes are more automated, and the dissipated perimeter makes it easy for traffic to bypass defensive measures. The threats, on the other hand, are just as sophisticated.

Security controls must evolve alongside this dynamic environment. But the traditional approach that works well on premises can't keep up with the speed of DevOps teams automating deployment of new infrastructure and deploying applications faster than ever.

While the market offers a variety of cloud security products, SecOps teams continue to struggle with security policy implementation and enforcement. The multitude of point solutions creates unnecessary work, as well as fragmenting visibility and leaving gaps in coverage. But how can you consolidate all those controls and gain a single source of truth that gives you a unified view of your environment?

The answer is cloud-native solutions. Purpose-built, cloud-native security tools were designed to meet the cloud security challenges. These solutions adapt to cloud changes dynamically, scale alongside cloud resources, and automate controls.

Strategic platform consolidation plays a critical role as well. When you can integrate visibility and control into a single system, you realize significant security benefits in terms of mean time to detect (MTTD) and mean time to respond (MTTR). Operationally, a security platform reduces integrations and ongoing operations costs while boosting security coverage. Now, you can apply this platform approach in the cloud — while ensuring that you meet the cloud's security prerequisites and that security can move as fast as your DevOps projects.

RESEARCH REPORT

How Log4Shell Changed Cloud Workload Security in 2022

Learn More ▶

Architecture Matters: Network Security Considerations in the Cloud

While cloud infrastructure is different from your on-premises one, the same multi-layered approach and network security functions are still relevant. However, the cloud's dynamic environment dictates different requirements for network security. And security provided by the cloud vendor does not adequately protect against threats at the cloud network level.

The primary considerations for a cloud security architecture center around the cloud's dynamic environment. Security solutions need to provide automated protections while learning and adapting to that environment. Cloud-native security inherits the cloud's attributes (elastic, automated, and consumption-based).

85% of surveyed cloud security leaders believe that poor cloud security tool integration slows down security processes and causes security lapses.[1]

Critical Components for Cloud Security Solutions

1. **Visibility into assets, traffic, and activity:** Visibility into your cloud environment is important — you need to know where you have workloads exposed to the internet, what network paths are open, and where other vulnerabilities exist. But that's not enough. Visibility into what's happening in the network is just as important as visibility into the security posture. Understanding the activities in the network, such as lateral movement and attacks, is what allows you to combat actual threats. This visibility is then used to create the policies that will protect those assets.

2. **Infrastructure-as-code (IaC):** Increasingly, DevOps teams are adopting IaC mechanisms to automate infrastructure provisioning and management as they build applications — and tools such as the open-source Terraform enable them to build the applications in a platform-agnostic way with just a few lines of code. By applying an IaC model to security and eliminating manual processes, you can integrate security into the development cycle. This tactic allows you to bake security into the application rather than adding it on top — and it speeds up deployment instead of slowing it down.

3 **Autoscaling:** For cloud deployments, autoscaling — often with elastic resources such as on-demand infrastructure — is an important component. This enables you, for example, to dynamically increase loads during peak times even when you don't know what kind of demand to anticipate. Likewise, security capabilities should autoscale along with the cloud workloads and the applications they are intended to protect. Cloud-native autoscaling allows security to work seamlessly with applications and you don't have to think about the complex logic of different parameters and thresholds.

4 **Workload identity and context:** By itself, visibility into the vast number of assets in the cloud doesn't have much meaning until you correlate the data between the traffic and assets such as IP addresses and applications. Traditional methods that worked in the data center, such as writing policies based on static IP addresses, don't work in the cloud because of its dynamic and elastic nature. A cloud security platform with integrated dynamic asset discovery and tagging in near-real time automatically finds the identity and contextual information for cloud assets. This enables you to both eliminate ineffective, broad-strokes security policies and better understand how well your policies are actually working.

5 **Self-healing:** When something breaks down in your cloud security infrastructure, you need to take care of the problem quickly, but manual work takes time. The self-healing functionality automatically identifies security failures and autonomously fixes them. This component reduces manual errors — improving your security effectiveness and efficiency — and enables you to focus your people resources on bigger priorities.

6 **Multi-cloud support:** Due to the differences in architecture and the lack of standard protections, each cloud environment requires its own approach to security. Managing security separately for individual clouds adds a layer of complexity that leads many organizations to accept compromises and weaker security compared to their data center. Multi-cloud support is a core requirement that allows the consolidation of security management across multiple clouds. It ensures your cloud security solution integrates with the native controls available from each provider, and eliminates the need for the IT or security team to deeply understand each individual provider's security architecture.

In addition to these six core components, consider the effort your cloud security tools will take to deploy and operate. Like any other cloud service, they should be fast and easy to roll out and manage, requiring minimal effort on your part.

Capabilities to Look for in Your Cloud Security

Many of the security functions you deploy on premises remain relevant in the cloud. The primary difference is that they need to meet the unique cloud requirements, as described in the components above.

- **Firewall:** In the cloud, the firewall defines the trust boundaries in your environment, separates trusted traffic from untrusted, and applies policy over what type of traffic you allow in your cloud network.
- **Data loss prevention (DLP):** DLP provides visibility and control into the movement of sensitive data in your cloud environment. Security policy based on context and content defines the thresholds of monitoring, alerting, and potentially blocking of unauthorized activity.
- **Intrusion detection/intrusion prevention system (IDS/IPS):** IDS/IPS provides real-time protection against network attacks, exploits, and exposures in application code and operating systems that workloads run on. IDS/IPS is not only a critical security control, but is often required for compliance and is instrumental in virtual patching against exploits of vulnerabilities such as Log4SHELL.
- **Egress filtering:** Controlling outbound destinations from cloud workloads prevents unauthorized connections (such as command-and-control communication) and data exfiltration from cloud applications.
- **Antivirus/antimalware (AV):** Malware often plays a key role in the attack lifecycle and ransomware, of course, can wreak havoc. AV detects and blocks these threats. Networks-based AV can be effective in detecting malware signatures without the need for host-based agents, which cause operational issues and may not be compatible with every piece of infrastructure.
- **Web application firewall (WAF):** A WAF provides additional security at the application level to defend against internet-borne (ingress) attacks, provide denial of service (DoS) protection, improve visibility into geolocation of users, and protect from malicious IPs.
- **TLS decryption:** You have to assume that cloud traffic is going to be encrypted, and you'll need to decrypt it for full visibility and inspection.

The pace of change in the cloud is fast, and security must keep up. But with hundreds or thousands of virtual public clouds, accounts, and applications, it's challenging to adapt security to the changes quickly and fight threats proactively. One way to solve this challenge is by implementing a platform that integrates all the critical security components, boosting your effectiveness and providing single-console management that ties visibility into advanced controls.

Why Virtual Network Security Appliances Fail in the Cloud

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

Organizations have used network security appliances in the data center for decades. While the natural inclination might be to continue this model in the cloud, the virtual appliance form factor is not well aligned with the dynamic nature of the cloud. The impact of adopting virtual appliances may include excessive cost, poor security coverage, and reduced agility for the business.

The disadvantages of virtual appliances include:

- **Operational complexity** — firewall providers supply unsupported scripts that require extensive cloud knowledge to correctly customize and maintain.
  Result: Excessive cost
- **Lack of cloud native workload identity** — application IDs are not supplied for PaaS services and association with cloud workloads must be done manually against static IPs due to the lack of tag-based policy.
  Result: Poor security coverage
- **Lack of cloud scale** — scale must be manually managed, which creates a chokepoint. Lack of adequate Terraform (IaC) support means that the security is not aligned with DevOps.
  Result: Reduced agility

Consolidate Solutions, Simplify Management with an Integrated Platform

Similar to the data center and your on-premises environment, the cloud requires a defense-in-depth strategy. No single control is foolproof and a layered approach helps you avoid a single point of failure.

97% of IT leaders view defense-in-depth as essential to the cloud.[1]

Managing multiple cloud security solutions, however, creates disadvantages such as fragmented visibility, operations, policy, and response; inconsistent policy enforcement; and slower threat response times. A multi-cloud security survey by Valtix found that the lack of unified visibility into security controls and policy across clouds creates more work for 82% of the surveyed organizations.[2] This is especially a challenge since many IT and security teams are already stretched thin due to the talent gap.

An integrated platform that incorporates all your cloud security components provides a single source of truth and enables the security function to match the dynamic nature of the cloud. A purpose-built platform does much more than simply consolidating your security to save costs — it eliminates the cracks that point tools create and allows IT and security teams to move faster, save time, and identify security gaps more holistically with a single policy and a single service chain.

Top Reasons to Consider an Integrated Approach

1. **Single policy management:** A defense-in-depth strategy creates overlapping controls at the various defense points. If you're writing separate policies for each of the point solutions, you're duplicating processes and spending additional cycles before the application can go live. An integrated platform eliminates the redundancy and gives you a single policy from which all your security functions operate, saving time, reducing complexity, and allowing you to enforce policies consistently across your entire environment.

2 **Lower latency and higher performance:** Decrypting traffic individually for each security control so you can perform inspections adds latency and degrades performance. This typically results in either security compromises (such as foregoing resource-intensive east-west traffic decryption) or poor end user experience. An integrated platform allows for a single-pass inspection where you only have to decrypt traffic once for all the controls.

3 **Improved overall effectiveness:** A platform automates many of your security processes, minimizing the risk of error and reducing overhead. By connecting visibility at multiple points of the attack lifecycle with the ability to take remediation action, integrated security platforms provide significant improvements to MTTD and MTTR.

The top three outcomes to expect from a platform model include:

#1	**Simplified business processes and user training** by eliminating the need to learn every vendor's security architecture and requirements
#2	**Reduced implementation and maintenance costs** by decreasing the work and resources required to deploy and maintain separate solutions
#3	**Lowered security and business risk** by identifying threats faster and automating mitigations to prevent business impact

Cloud security platforms are based in the cloud and are typically offered as a service. They scale on demand to provide additional capacity when you need it and integrate with various third-party tools such as open-source automation solutions. A robust platform provides all the critical security capabilities while meeting the unique cloud components discussed earlier.

Valtix: Multi-Cloud Network Security for a Cloud-First World

Organizations view the public cloud as an essential resource for supporting their digital transformation initiatives. The last couple of years have demonstrated that agile businesses can quickly adapt in some of the most challenging and uncertain business conditions — and only the cloud provides this kind of speed. But traditional security models don't scale to the cloud.

That's where Valtix comes in. Agile, scalable, comprehensive, and robust, the purpose-built Valtix Platform delivers an end-to-end, integrated approach to cloud network security. The cloud-native platform enables your security to move at the same speed as your cloud operations by combining core cloud network security controls and seamlessly adapting to dynamic cloud environments.

Offered as a pay-as-you-go service model, the platform works in three steps:

1. **Discover** — identify cloud assets and security gaps in seconds without deploying any agents.
2. **Deploy** — enable the Valtix Cloud Gateway with one click, either in the Valtix console or through Terraform.
3. **Defend** — configure adaptable network security based on your requirements.

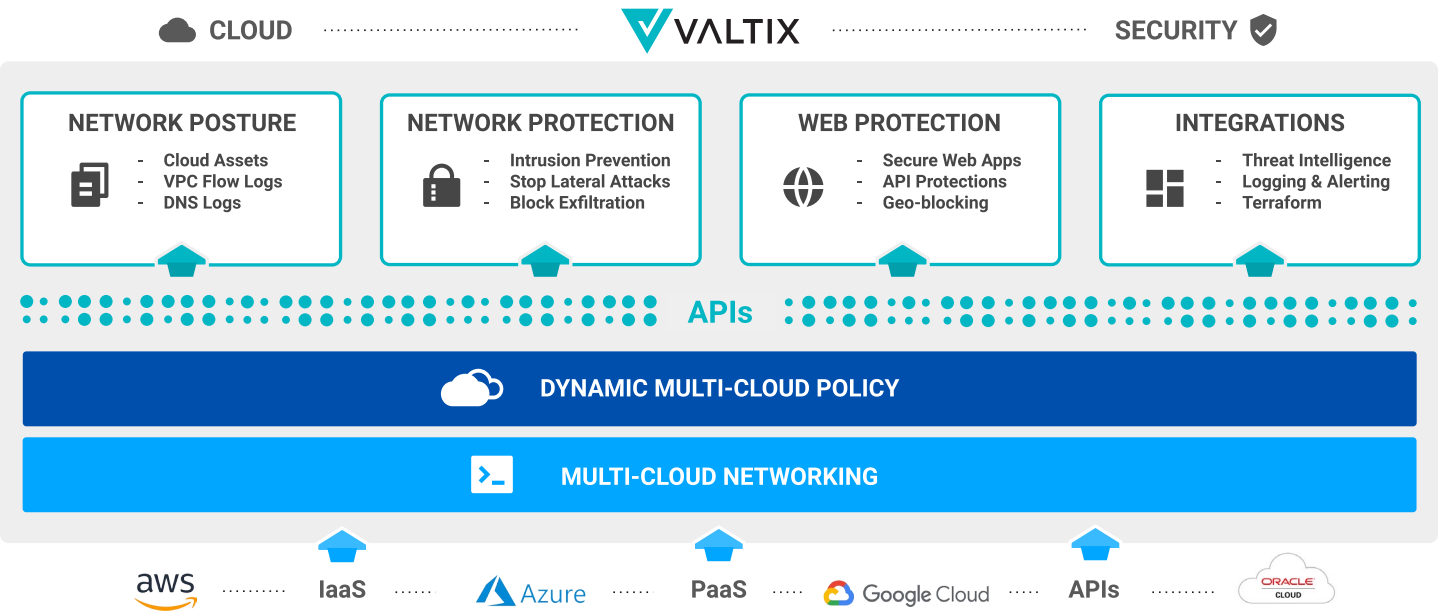
Core Valtix Platform Capabilities

Network posture: Gain unified visibility into your entire cloud network through continuous asset discovery and inventory, assess open network paths, and identify suspicious traffic. Valtix also surfaces gaps in your network security coverage and offers recommendations for closing them.

Cloud network protection: Valtix delivers advanced network protection for multi-cloud environments, securing ingress, egress, and east-west traffic. The network protection enables you to detect and block malicious or prohibited activity, prevent lateral movement, and meet compliance requirements. Capabilities include firewall, IPS/IDS, antivirus/antimalware, DLP, and egress filtering.

Web protection: An integrated WAF protects your web applications and APIs from external threats. By deploying and managing the WAF alongside network security controls, you improve security through a single-policy framework. The WAF also provides integrated threat intelligence, advanced security rule sets, and geolocation-based controls.

Integrations: Valtix integrates out of the box with several cloud services, such as Terraform, ServiceNow, and Splunk. You can fully automate and integrate the platform with your IaC initiatives, enable centralized workflows for SecOps teams, and enrich your extended detection and response (XDR) activities. The platform also integrates threat intelligence feeds and third-party solutions such as SIEM and SOAR.



Benefits of Implementing the Valtix Platform

Among IT leaders surveyed by Valtix, 96% said their job would be easier if they had one console for managing security across clouds. Valtix delivers this single-view management while continuously discovering new cloud assets and changes, associating tag-based business context, and automatically applying security policies.

Benefits of Valtix include:

- **Fast deployment** — rapid time to value with flexible delivery across many cloud security architectures (centralized, distributed, or hybrid)
- **Comprehensive, advanced layered defenses** — proactive defense-in-depth through advanced, cloud-native security controls
- **On-demand scalability** — continuous adaptation, in seconds, to new assets and changes to existing apps
- **Automation** — 1-click deployment via SaaS console, IaC with Terraform, and automated security policy based on context through tags
- **Reduced maintenance** — no scripts or complicated appliances to maintain
- **Improved productivity** — 10X productivity boost thanks to consolidated workflows, easy deployment, and minimal upkeep

Quantifying the Impact

Although every organization is different, most Valtix customers derive significant business, financial, and risk reduction benefits. They include:

- **Lower operating expenses** — decrease your SIEM costs, eliminate point tools and cloud-specific services, and lower your compliance burdens to cut down on operating expenditures.
  Potential benefit: $100,000s – $1M+
- **Time to market** — implement security in minutes rather than weeks so you can drastically shorten your time to market and innovate ahead of your competition, gain competitive differentiation faster, and increase revenues by capturing more sales.
  Potential benefit: $1M+
- **Lower risk** – reduce your implementation effort, roll out security faster, improve coverage, mitigate zero day exposure, and accelerate incident response time to reduce your overall security risks.
  Potential benefit: Priceless

Streamline Security Operations

Cloud DevOps teams move fast, and SecOps teams are struggling to keep up. While network telemetry in the cloud is essential to detecting, investigating, and containing threats, many organizations are either not collecting it or relying on traditional methods that don't meet the unique cloud requirements.

Valtix supports SecOps through centralized workflows and integration with security tools such as SIEM and SOAR. Alerts and logs generated in the platform can be forwarded for analysis, correlation, and investigation, as well as used for enabling incident response workflows. Valtix enables SecOps to adapt to the changes of the cloud as fast as DevOps can.

Enable Zero Trust Security with Valtix

Zero trust is an emerging security model that has become best practice across many industries — and increasingly, a government mandate. This approach shifts defenses from static, network-based perimeters to protect your resources, assets, and applications anywhere.

Zero trust assumes that no connection or user can be trusted implicitly regardless of location or application ownership. This model is especially effective in the cloud, where the assumption is that nothing is secure, even a trusted entity within the network.

Valtix enables an appliance-free, agentless zero trust approach through a microsegmentation architecture that prevents lateral movement across your network. You can define granular policies to enable least privilege access between (east-west) and to or from workloads (north-south) in AWS, Azure, GCP, and OCI. Segmentation is automatic across all connections and clouds with dynamic policy and cloud-native workload identity.

Advanced Security That Doesn't Slow Down Cloud Agility

As you continue to take advantage of the cloud's flexibility and scalability, it's critical to mitigate the security risks in the same way the cloud works — quickly, dynamically, and at scale. A platform approach solves many of the security challenges that either force organizations to compromise security or prevent them from growing their cloud initiatives.

The Valtix Platform operationalizes your cloud security so you can gain operational freedom and focus your resources where they matter the most — on your business outcomes rather than on a never-ending stream of security tasks. With Valtix, you can balance security with flexibility so you can meet your business objectives and continue to adapt quickly to the evolving business environment.

The biggest mistake that organizations make is choosing cloud security that negates the cloud's benefits. If you value the speed, agility, and competitive advantage that the cloud offers, ensure your cloud security delivers the same.

Tour the Product

VALTIX

Request Demo

Ready to get started?
Schedule a demo at **Valtix.com**

About Valtix

Valtix is on a mission to enable organizations with security at the speed of the cloud. Deployable in just 5 minutes, Valtix was built to combine robust multi-cloud security with cloud-first simplicity and on-demand scale. Powered by a cloud-native architecture, Valtix provides an innovative approach to cloud security called Dynamic Multi-Cloud Policy™, which links continuous visibility with advanced control. The result: security that is more effective, adaptable to change, 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. Valtix has been recognized as an innovator in numerous industry awards including 2021 top honors in the "Next-Gen in Cloud Security" from Cyber Defense Magazine, SINET-16 Innovator recognition, and inclusion in Gartner's Cool Vendors in Cloud Networking report.

Sources:

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

2 "The 2022 Multicloud Security Report," Valtix, 2022