VALTIX

CREATING A MULTICLOUD SECURITY OPERATING MODEL

Why Going Cloud-Native Is Essential to Closing Your Multi-Cloud Security Gaps

MULTICLOUD IS UBIQUITOUS. SECURITY IS NOT.

Multi-cloud adoption has accelerated in recent years. In 2021, 92% of organizations of all sizes surveyed by Flexera[1] had a multi-cloud strategy, with public cloud spend comprising a bigger slice of IT budgets than in previous years.

Undoubtedly, organizations have embraced all that multi-cloud environments have to offer. While the majority have already invested significantly into more than one cloud to support digital transformation and other initiatives, many plan additional investments to further enable their digital business.[2]

Multi-cloud success, however, remains elusive for many organizations. Among midsize companies, for example, only 50% report that multi-cloud has helped achieve business goals, according to a 2021 survey by HashiCorp.[3]

Studies have called out cost management, governance, and visibility as common barriers to adoption and deployment. But one factor that consistently lingers at the top is security—remaining a struggle even for advanced users as their adoption reaches maturity. In a recent Valtix survey, 51% of IT leaders agreed or strongly agreed that their company doesn't want to expand to additional clouds because of the security complexities.[4]

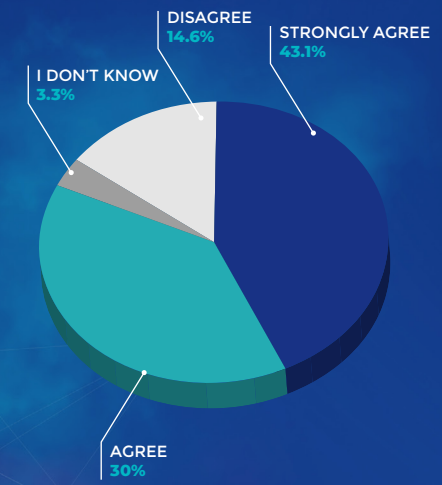
One driver behind the challenges is the expectation that you can simply extend your data center or on-prem security framework into the cloud. However, to solve the security complexities associated with multi-cloud environments, your strategy needs to adapt to the dynamic environment with a cloud-first approach.

This white paper recommends a security model that can help you advance on your multi-cloud journey at the speed of the cloud—and your business.

[1] "2021 State of the Cloud Report," Flexera, March 2021
[2] "Digital Transformation Index 2020," Dell Technologies, 2020
[3] "HashiCorp State of Cloud Strategy Survey," HashiCorp, 2021
[4] "The 2022 Multi-Cloud Security Report," Valtix, 2022
[5] "HashiCorp State of Cloud Strategy Survey," HashiCorp, 2021
[6] "2020 IDG Cloud Computing Survey," IDG
[7] "Survey: Security Public Cloud Infrastructure," Tripwire, July 2021
[8] "2021 State of the Cloud Report," Flexera, March 2021
[9] "HashiCorp State of Cloud Strategy Survey," HashiCorp, 2021

Agree or Disagree?

The complexity of implementing and managing multi-cloud security policy **SLOWS DOWN BUSINESS AGILITY**



SOURCE: VALTIX 2022 MULTICLOUD SECURITY REPORT (Link)

Multi-Cloud Adoption and Barriers

- 76% of midsize companies employ multiple clouds[5]
- 79% of organizations experience significant downsides to multi-cloud models (such as complexity and costs)[6]
- 98% of organizations say multi-cloud creates additional security challenges[7]
- Security is the No. 1 multi-cloud challenge for 81% of organizations[8]
- Staff and skilling issues are the most significant challenge for every component of cloud (provisioning, networking, security, app deployment)[9]

ADDRESSING CLOUD SECURITY PROACTIVELY

***72%** of IT leaders say security within their multi-cloud strategy is "definitely" a top priority for their team.*[10]

In a perfect world, organizations would move to a multi-cloud model methodically and strategically. This would allow them to think proactively about security instead of reacting to the new risks.

In reality, many implemented a bottoms-up, decentralized—perhaps even chaotic—approach to initial adoption. Driven by the need for speed and functionality, they deployed whatever made sense at the time—often in siloes, without consulting other teams or centralizing decisions.

While these organizations will have to work harder now on proactive security, they don't have a choice. And the risks are growing rapidly, which means now is the time to act.

*Cloud vulnerabilities have increased **150%** over the last five years.* [11]

The good news is that many IT pros already understand that they can't implement security in the cloud the same way they did on premises. In the Valtix survey, 89% of the respondents said they saw cloud security differently in those two environments.

Extending on-prem security into the cloud is not the best approach because:

- Legacy security architectures aren't flexible enough to accommodate the dynamic, service-based, software-defined public cloud environments.
- Security in the cloud needs to inherently adapt to the dynamic nature of workloads and applications and automatically scale to provide protection.
- The disparate features among the varied application architectures, cloud network constructs, and built-in security tools create an inconsistent security posture across your multiple clouds, leaving gaps in your defenses.

To address security proactively, consider purpose-built, cloud-native solutions that consolidate security management of all your clouds. These solutions are designed to provide end-to-end visibility and control, advanced threat prevention and defense in a highly dynamic environment—from a single platform.

EACH CLOUD REQUIRES A **DIFFERENT APPROACH TO SECURE**

[10] "The 2022 Multi-Cloud Security Report," Valtix, November 2021

[11] "2021 IBM Security X-Force Cloud Threat Landscape Report," IBM Security, 2021

THE CHALLENGES OF MULTICLOUD SECURITY

The laundry list of cloud threats is long and diverse. To name just a few examples:

- Botnets
- Zero-day exploits
- Cryptomining
- Malware
- Malicious insiders
- Ransomware and lateral movement of threats

Considering the breadth and the magnitude of the threats, it's not surprising that 73% of organizations are very or extremely concerned about cloud security.[12]

> ***67%** of cybersecurity professionals see misconfiguration of the cloud platform or wrong setup as the biggest security threat in the public cloud.*[15]

> *Nearly **3 out of 5** senior executives are concerned about vulnerabilities within their companies' public clouds.*[16]

The risk of data breaches and data loss command the most attention, given that 80% of organizations have faced at least one cloud-related data breach in the previous 18 months.[13] And these data breaches are costly:

- The average data breach in a public cloud environment is $4.8 million, according to IBM Security's latest "Cost of a Data Breach Report."[14]
- The average cost of a data breach across the board is lower, $4.24 million.

While navigating the cloud threat landscape, organizations must grapple with numerous security challenges, including:

- The complexities—and the gray areas and vagaries—of the shared responsibility model
- Risks that are unique to the cloud, such as reduced visibility and control
- The inherent open model of the cloud, which requires additional considerations
- The inconsistent architecture and infrastructure of the various cloud environments
- Additional issues common across the board, such as talent shortage and compliance

Many of these aspects require granular expertise—not only in cloud networking and security but also in each cloud provider's product offerings and services, architecture, automation, and security tools—compounding the challenge.

12 " Cloud Security Report," Cybersecurity Insiders/Fortinet, 2021
13 "Top Identity and Data Access Risks," Ermetic/IDC, June 2020
14 "Cost of a Data Breach Report," IBM Security/Ponemon Institute, 2021
15 "Cloud Security Report," Cybersecurity Insiders/Fortinet, 2021
16 "C-Suite Perspectives: From Defense to Offense," Radware, 2019

THE SHARED RESPONSIBILITY MODEL: COMPLEXITIES, VAGARIES, INFLEXIBILITY

The shared security responsibility model of the public cloud keeps security teams on their toes. Providers typically offer guidelines, but in practice you can't rely on them completely—and the lines sometimes appear fuzzy. This became especially evident in light of recent exploits we've seen within cloud provider services, which required the end users to mitigate while waiting for a fix.

In a traditional service outsourcing model, your provider would work with your team to clearly define the boundaries. That's not the case in the cloud.

Where things get even more challenging is in the constant parade of updates and new services from providers. They introduce dozens of services and hundreds of new features every year, along with numerous updates. Developers eagerly consume the services because they solve specific problems or add new capabilities. The rapid pace of change makes their job easier—and the security team's job harder.

This throws security teams into a perpetual cycle of catch-up, trying to figure out the implications of each change. Multiply this challenge by the number of clouds you've deployed and the problem is quickly exacerbated.

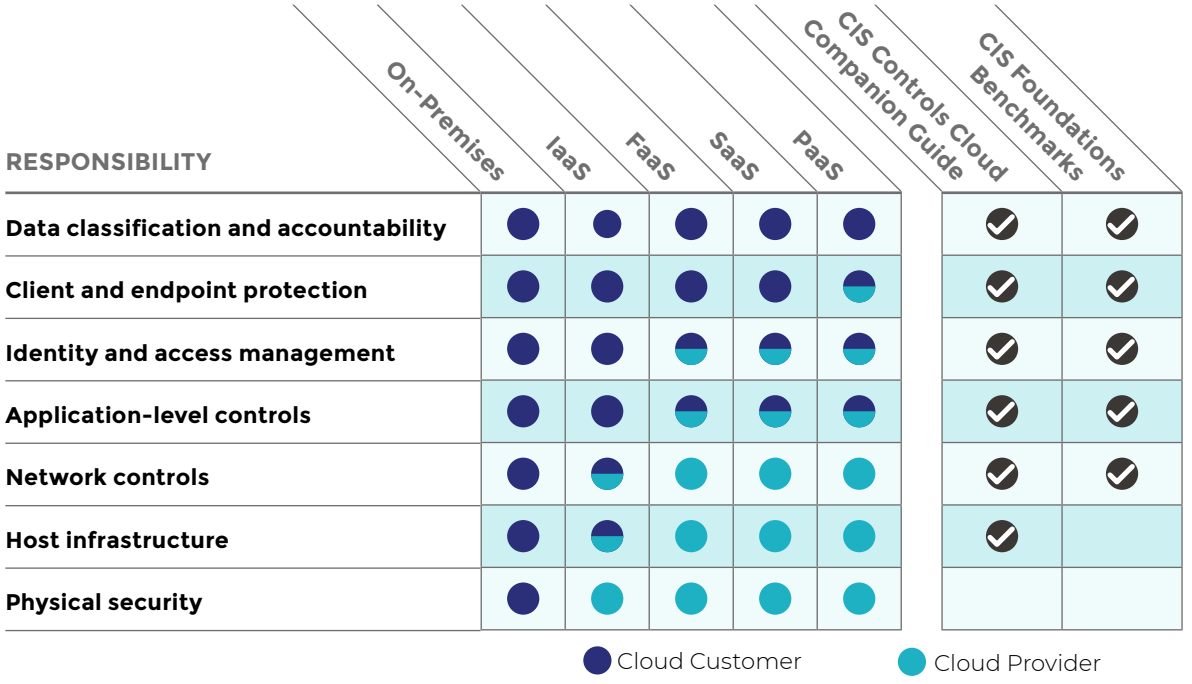
OTHER CHALLENGES

Unique cloud security risks: Reduced visibility and control are common problems, with 53% of surveyed cybersecurity professionals identifying lack of visibility and 46% calling out inadequate control as their top barrier to adoption.[17] Other risks include insecure APIs and lack of a centralized view across multi-cloud.

The talent gap: The cybersecurity industry has grappled with talent shortage for years, with the latest data showing a gap of 3.1 million security workers globally in 2020.[18] Provider-specific security requires deep expertise with each cloud's configurations, intensifying the talent issue.

Policy enforcement: The variations in controls in individual clouds and app architectures result in inconsistent policy enforcement across your environment, leading to gaps in protection and reduced security posture.

***3 Most Common** Ways Bad Actors Access Cloud Environments:*[19]
- *Password spraying*
- *Exploited software vulnerabilities*
- *Cloud deployment misconfigurations*



[17] "Cloud Security Report," Cybersecurity Insiders/Fortinet, 2021
[18] "(ISC)2 Cybersecurity Workforce Study," (ISC)2, 2020
[19] 2021 IBM Security X-Force Cloud Threat Landscape Report," IBM Security, 2021

BUILDING **LAYERED DEFENSES** IN THE CLOUD

Although your cloud architecture and security approach are different from on-prem, the tenet of multi-layered security still applies. There's no one-size-fits all solution that covers all the threat vectors and types of attacks. When building out your security layers, consider capabilities such as:

- Visibility into all your assets (apps, APIs, workloads, etc.) across all your clouds, as well as into your security monitoring and whether it's working as expected
- Cloud network security, such as firewall, data loss protection (DLP), workload segmentation, and intrusion detection/intrusion prevention systems (IDS/IPS)
- Protection against web threats, such as web application firewall (WAF) and malicious IP blocking
- Context-aware security across app lifecycle (dev, test, prod) and type of apps (general, sensitive, compliance)

Extending these security layers from the data center or bolting them on top of your architecture is ineffective and introduces new problems, such as orchestrating and automating the tools across multi-cloud.

Cloud-native security solutions:

- Offer advantages such agility, scalability, and elasticity
- Work seamlessly with your cloud apps
- Enable continuous discovery of new apps and infrastructure and automatic policy based on app context

[20] "Survey: Security Public Cloud Infrastructure," Tripwire, July 2021

*Only **21% of IT security teams** have a centralized view across all their cloud accounts.*[20]

IMPLEMENT ACTIVE DEFENSE

Cloud vulnerabilities are one of the biggest challenges for security teams. Consequently, these teams devote much of their time to patching. But managing vulnerabilities alone will not protect you against zero-day threats. By the time a vendor knows about a new threat and creates a patch, it may be too late.

Just like on-prem, multi-cloud needs both reactive and proactive defenses. Active defense enables you to block attacks, restrict unauthorized access to assets, and defend against new and emerging threats. The goal should be to break the attack kill chain in multiple places and not rely on a single point of failure in your defenses. For example, to stop an attacker on a breached server, a malicious insider, or a ransomware attack, an effective last stop is to restrict all outbound traffic to known categories of sites, domains, and URLs.

Consider a Zero Trust Approach

An emerging model, zero trust shifts defenses from static, network-based perimeters to protect resources, assets, and applications anywhere. By assuming no connection or user can be trusted, regardless of location, zero trust continuously and dynamically authenticates and authorizes access and enables you to strictly enforce policy-based controls. One way to implement zero trust is through a micro-segmentation architecture, preventing lateral movement across your network.

CLOUD SECURITY TECHNOLOGIES: BENEFITS AND DISADVANTAGES

Cloud security solutions fall into two main buckets: securing users and securing apps/workloads. For user security, security teams typically look to technology such as a cloud access security broker (CASB). Organizations are running an increasing number of workloads in the cloud—some more than half—so we'll focus on three technologies that cover the app side of things:

- Cloud workload protection platforms
- Cloud security posture management
- Cloud network security platforms

CLOUD WORKLOAD PROTECTION PLATFORMS (CWPP)

As the name implies, CWPP secures workloads in multi-cloud with an agent deployed on each workload. These solutions grew from the need to protect workloads as organizations began migrating to IaaS because the security requirements of cloud workloads are different from traditional IT systems.

In short, regardless of the workloads' location and granularity, CWPP protects them from attacks. Because it's agent-based, CWPP is difficult to deploy and manage across multiple clouds. This technology may be best for hybrid environments that include virtual machines, as VMs require you to run specific code from the software vendor for system-level security.

PROS:

- Includes capabilities such as network visibility, firewalls, and identity-based segmentation; some solutions offer controls such as application whitelisting.
- Enables you to manage workload vulnerabilities and harden configurations.

CONS:

- Not all vendors' CWPP solutions extend security to containers and microservices.
- Installing and maintaining agents on every asset slows down deployment, adds costs, and may impact performance.

BOTTOM LINE:

Many organizations have been deploying CWPP together with cloud security posture management, but CWPP is no longer an essential component of your cloud security stack because the needs of multi-cloud have outgrown CWPP technology.

As we'll discuss later, there's a better way.

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

A serverless solution, CSPM protects primarily against vulnerabilities such as misconfigurations. While cloud providers offer some basic risk assessment and configuration, CSPM delivers both more advanced controls and multi-cloud capabilities. Additionally, the technology helps solve challenges related to the dynamic nature of multi-cloud and visibility due to cloud sprawl.

CSPM discovers new assets and then assesses their risks and security settings. It provides consistent policy enforcement based on your organization's security policies, as well as security frameworks (such as NIST) and regulatory compliance requirements.

PROS:

- Enables you to continually prevent, detect, and respond to infrastructure risks, such as excessive access permissions, misconfigurations, exposed APIs, and weak authentication.
- Provides more granular controls than built-in provider tools while automating various tasks and helping you to enforce policies consistently.

CONS:

- Doesn't proactively stop attacks or exfiltration—which means it won't protect you from threats like malware and ransomware.
- Doesn't detect lateral movement once a threat is in your environment—especially from frontend to backend and other connected systems.

BOTTOM LINE:

CSPM is a requirement for protecting your multi-cloud against human mistakes, oversights, and missed updates, and for allowing you to take immediate action. But it's not sufficient as a standalone tool. You need to do a lot more than patching, managing configurations, and addressing vulnerabilities. CSPM only tells you the risks based on your configurations—it doesn't tell you what's actually happening in your network, nor does it provide any active defense.

CLOUD NETWORK SECURITY PLATFORM (CNSP)

A newer category of cloud security, CNSP offers security capabilities as a cloud service. The solution can provide an abstraction layer that simplifies multi-cloud security with a unified management console so you can apply one policy across multiple clouds. Additionally, CNSP offers full visibility of security events across a complex environment with correlation to specific applications and policies.

An agentless solution, CNSP delivers asset discovery, network protection, and web protection. It defends your organization against threats that require east-west movement, such as ransomware; detects malicious behaviors based on attack patterns; and prevents data exfiltration.

Why You Need Network Security in the Cloud

Network security is critical in the cloud because it gives you proactive security that is independent of the underlying application infrastructure or cloud provider. While you also need compliance and governance tools, along with continuous cloud monitoring, those solutions won't protect you against real-time attacks or data exfiltration.

PROS:

- Cloud network security is independent of the underlying application infrastructure (containers, VMs, etc.) and therefore provides a common point of security and consistent multi-cloud architecture.
- Network security techniques such as network-based segmentation, web app firewall, and intrusion prevention provide a strong defense against the exploitation of vulnerabilities.
- Allows implementing context-aware security based on the workload identity.

CONS:

- Virtual appliance-based solutions may be complicated and time-consuming to implement correctly.
- Each cloud provider makes cloud network security services available, but these can be complicated and costly to implement. They also are specific to that cloud provider, thus being prohibitive for multi-cloud.

BOTTOM LINE:

CNSP complements CSPM by adding protection against other serious threats to give you a complete stack for securing apps and workloads. A third-party, cloud-native CNSP overcomes the technology challenges of virtual appliance based or cloud provider specific services to offer robust, layered defenses, along with fast deployment that takes only a few minutes across a multi-cloud infrastructure.

REQUIREMENTS TO CONSIDER IN A CLOUD SECURITY SOLUTION

Although cloud security solutions have different functionalities based on their category, they share a set of common criteria, such as deployment and management simplicity. When evaluating a vendor's solution, consider the following aspects:

Security Capabilities:

Security capabilities vary broadly for each solution, even within the same security category. For robust, unified security, look for the following top capabilities in a single solution:

- **Continuous visibility:** To detect malicious activities such as data exfiltration, you need to combine your cloud asset information and threat intelligence with complete visibility into all traffic flows, including inbound from and outbound to the internet, east-west, and to PaaS services.
- **Comprehensiveness:** A thorough and comprehensive, end-to-end platform will reduce or eliminate the need for multiple point products and enable you to consolidate your cloud security. Look for critical capabilities such as dynamic policy enforcement, identity-based segmentation, network protection, and web protection.
- **Active defense capabilities:** If your security only allows you to react to threats rather than proactively stop them, your team will always remain at least one step behind the adversary. In the past, active defense required an agent-based solution. Newer solutions are agentless, reducing deployment and maintenance challenges.

Cloud Scalability:

Your business requirements and environment change, and security needs to scale up or down quickly along with the resources it protects. The cloud security platform should automatically perform tasks such as discovering new assets and applying context-based policy—so your team doesn't have to constantly worry about operating the tool across multiple clouds, regions, and accounts.

Ease and Speed of Deployment:

Your cloud security solution shouldn't add to the complexities of multi-cloud, yet many vendors' products are difficult and time-consuming to deploy across an organization's public cloud infrastructure. Look for a turnkey solution that is simple and fast to implement and works natively in your environment. This will eliminate the need for admins to manually adapt the environment—instead, the solution "learns" the environment via the APIs in that cloud.

Single Policy Framework:

A centralized control plane across disparate clouds enables you to enforce granular security policies consistently from one console, simplifying multi-cloud management. To achieve this, the security solution should provide an abstraction layer that decouples control and dataplane.

ADOPT END-TO-END, CLOUD-NATIVE SECURITY WITH VALTIX

Valtix solves the complexities of multi-cloud security with a network security platform delivered as a service. Agile, scalable, comprehensive, and robust, this platform supports multi-cloud environments with specific capability for AWS, Azure, GCP, and OCI.

Valtix delivers:

- Layered, proactive defense through advanced security controls (including firewall, WAF, DLP, and IDS/IPS)
- Fast and simple deployment in minutes without additional infrastructure
- Continuous, dynamic, real-time visibility into all your cloud apps and infrastructure
- A single, dynamic policy framework for consistent, automatic policy enforcement across multi-cloud
- A flexible, open platform that integrates threat intelligence feeds and third-party solutions such as SIEM and SOAR

Today's IT and DevOps teams move fast to support digital transformations and other initiatives that keep your business competitive. Valtix helps your teams accelerate successful multi-cloud adoption cost-effectively and with the skilled resources you already have, without compromising on cloud security.

Solve Multi-Cloud Complexities Strategically

Multi-cloud adoption is no longer a choice—it's an essential element in the fast-paced, modern business environment where agility impacts the success of your business. Without strategically addressing the complexities of multi-cloud, you won't reap the full benefits of this model.

Implementing security adds to those complexities, creating yet another barrier to full implementation. You can overcome the hurdles by shifting to a cloud-first mentality—and this requires finding partners that can fulfill your business need for agility and speed.

VALTIX NUMBERS THAT MATTER

5 MINUTES TO DEPLOY
Cloud-first simplicity to deploy security and policy across clouds or accounts

100% CLOUD COVERAGE
Connects discovery to defense so that every account, app & API is secured

ZERO AGENTS OR APPLIANCES
No agents or infrastructure to maintain means fewer outages and lower costs

30 SECONDS TO ADAPT
Adapts dynamically to new apps and changes to existing apps

10X PRODUCTIVITY
Cloud-first simplicity to deploy security and policy across clouds or accounts

LOW LATENCY
Cloud-native approach and single-pass architecture doesn't degrade app performance

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 by 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.*

Get started with a free trial and a cloud visibility report at **Valtix.com**.

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