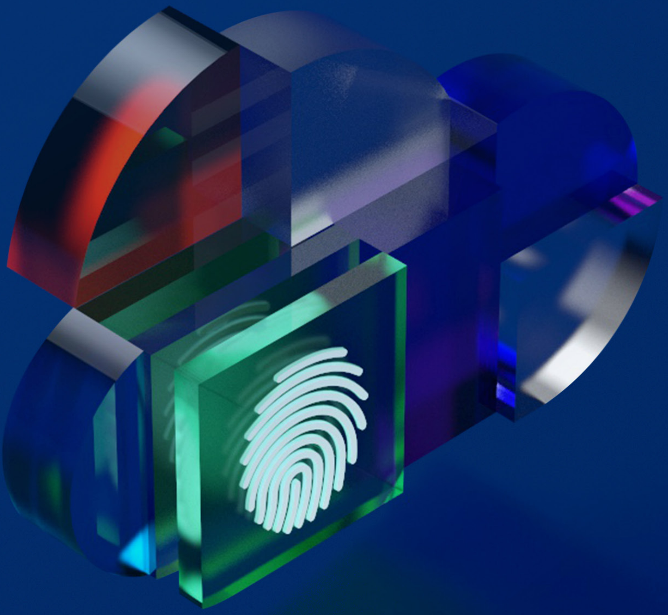
Kong

EBOOK

# Security in a Multi-Cloud World



# Content

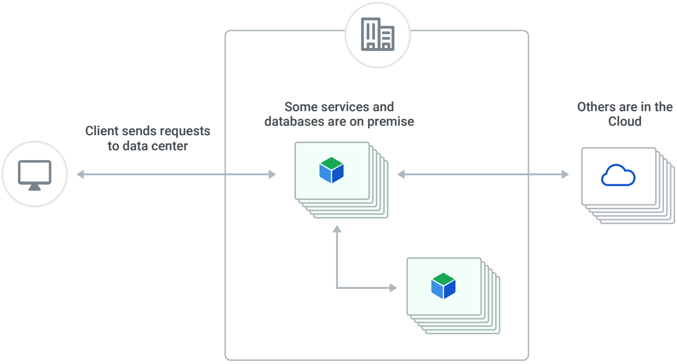
# Security in a Multi-Cloud World

## Part 1: Opportunity and Responsibility

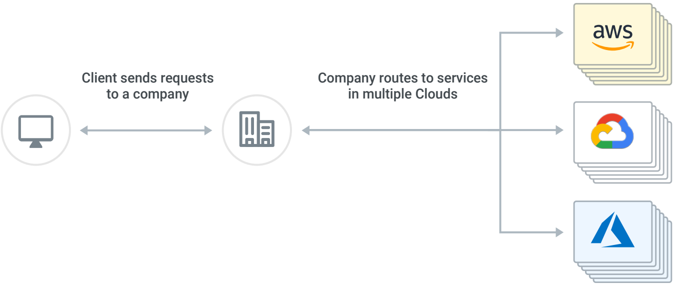
### Introduction

Companies continue to adopt the Cloud thanks to the availability, flexibility and security it offers. Those that are fortunate enough to start in the Cloud have an incredible advantage in that they do not need to maintain and migrate legacy systems.

Although the Cloud has its benefits, for many large organizations, it's difficult to lift and shift all workloads completely to the Cloud. This difficulty results in multiple different environments to maintain. Since security is easier to enforce with visibility and consistency across systems, the hybrid model poses a challenge since consistency is not always achievable.


Client sends requests to data center
Some services and databases are on premise
Others are in the Cloud

To further complicate matters, many enterprises use more than one cloud provider. The downside to this approach (from a security perspective) is that security controls now need to be wedged into environments with different toolsets, even if they are conceptually similar. The ecosystem of services in each cloud demands increasing levels of specialization, forcing companies to rely more on talented people and less on the universal process.


Client sends requests to a company
Company routes to services in multiple Clouds
aws

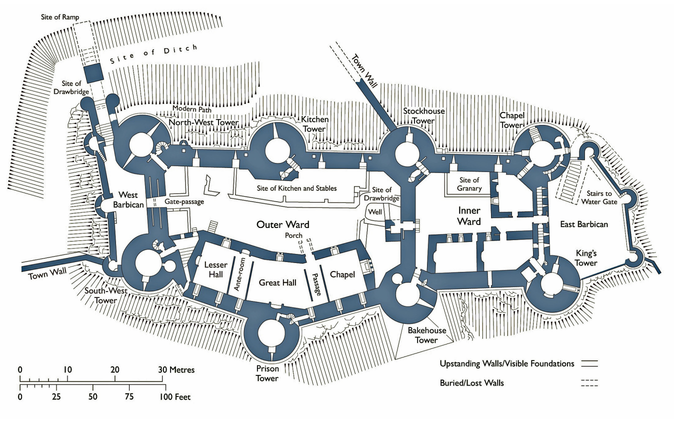
At the lowest level of abstraction, the security considerations that face the Cloud are hardly new—application, network and host security are still discernible and addressable in much the same way as they would be on premise.

What has changed is that each of these considerations needs to be addressed in different environments with different tooling, multiple sets of policy and a governance nightmare. If a security team is struggling to keep up with audit and security tickets across multiple cloud providers, the task of creating an overarching security strategy stays on the backburner.

Ten years ago, people were debating whether to move to the Cloud. Five years ago, moving to the Cloud became a fact of life—but so did the reality that security could ruin everything. Now we stand at a critical juncture.

## Security with a Builder’s Mentality

Hundreds of years ago, civil architects were often military engineers by default. Security was of central importance to medieval and early modern urban and structural design in ways that we can extend to how we design distributed systems today.

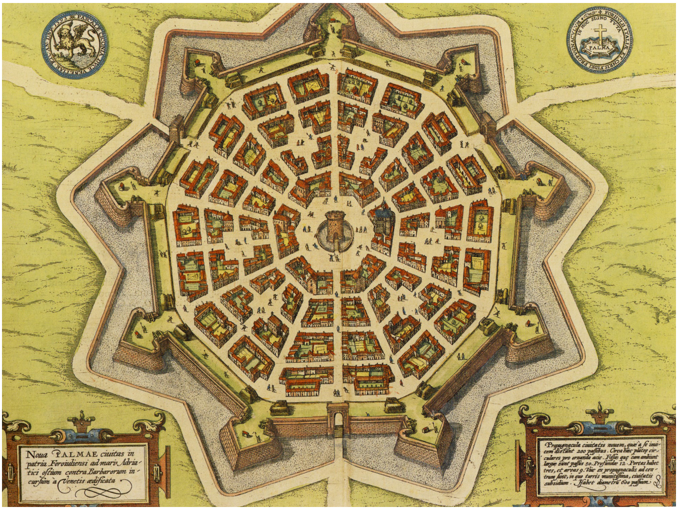


Source: https://commons.wikimedia.org/wiki/File:Conwy_Castle_plan.jpg

Early builders had concerns with the movement of people and storage of goods similar to the ones we have about the movement and storage of data. Beyond traffic flow and load-bearing, medieval architects also focused on the resilience and security of their designs. As early architects discovered and anticipated new threats, they needed to update their paradigms.

In the late medieval period, cannons prominently entered the battlefield. Suddenly, high walls became easy to knock down. Similarly, when we moved from mainframes to the client-server paradigm, we were immediately plagued by the prevalence of session hijacking, in which attackers could intercept our communications with the server, stealing our information or inserting their own.

To respond to the new threat of cannons, medieval architecture underwent a massive shift: low, long ramparts with distributed angles replaced the older style of flat, high walls. The famous “star fortress” was a solution that lasted for centuries. To respond to session hijacking, in the past five years, we have rapidly seen the emergence of our own “star fortress” with the prevalence of site-wide TLS. Google Chrome’s use of the “Not Secure” warning has dramatically changed the behavior of companies hosting websites, such that even static sites such as the New York Times use TLS.

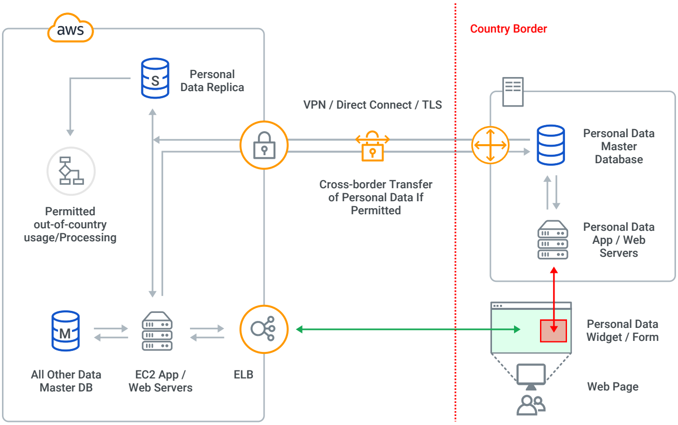

Noua PALMAE ciuitas in patria Foroiulienſi ad maris Adriatici oſtium contra Barbarorum incurſum à Venetis ædificata
Propugnacula ciuitatis nouem, quæ à ſe inuicem diſtant 200 paſſibus. Circa hæc plateę circulares pro ornanda acie. Foſſæ quę eam ambiunt largæ ſunt paſſus 30. Profundæ 12. Portas habet tres, et areas 9. Viæ ex propugnaculis ad centrum ſunt, in quo turris munitiſſima, ciuitatis ſubſidium. Habet diametrũ 600 paſſuum

Source: https://en.wikipedia.org/wiki/Bastion_fort#/media/File:Palmanova1600.jpg

With the much later appearance of the airplane, defensive measures moved from walls around cities and forts to RADAR around national airspace. The move to the Cloud has also led to yet another massive shift in security and privacy concerns. Business leaders, in particular, need to develop an understanding of where responsibility lies and how to handle their journey to the Cloud. Borders, secrets, vaults and walls are still the means of safely enduring this journey, but the rapid multiplicity of environments is the single most pressing challenge in the builder's mindset.

Compare the borders of data centers and the Cloud to the borders of countries. There are ports of entry, and there is a process of verifying who and what is traversing the border. More pertinently, though, there are different laws and customs behind each boundary. Even if there is a commonality between these rules, they may appear in different languages with different nuances and various means of enforcement. As a result, it becomes increasingly complex to maintain a universal law across borders.

Now consider that oftentimes, those literal and figurative borders coincide and that the security concerns within networks map to privacy concerns for citizens in a global economy.


aws
Country Border
Personal Data Replica
VPN / Direct Connect / TLS
Permitted out-of-country usage/Processing
Cross-border Transfer of Personal Data If Permitted
Personal Data Master Database
Personal Data App / Web Servers
All Other Data Master DB
EC2 App / Web Servers
ELB
Personal Data Widget / Form
Web Page

Source: https://aws.amazon.com/blogs/aws/in-country-storage-of-personal-data/

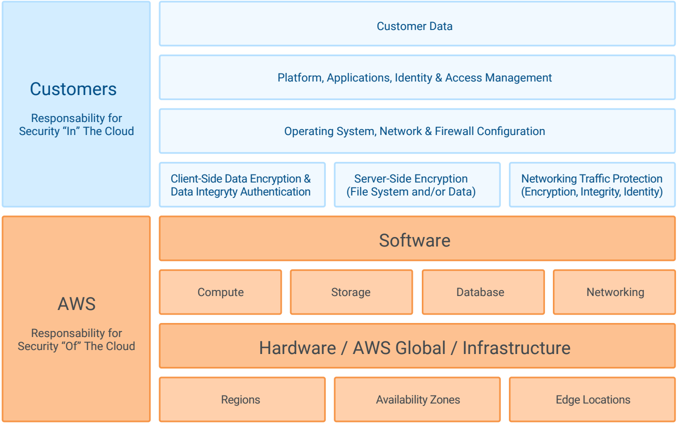
# Part 2: Mixed Environments

## Responsibility in the Cloud

The Cloud has saved large enterprises millions of dollars in security spending. It has made it possible for countless small businesses to enjoy the same benefits that would otherwise be impossible to obtain on their own. The reason is that Cloud Service Providers (CSPs) have an incredible economic incentive to keep their customers as safe as possible.
Consider the allure of government contracts such as the Joint Enterprise Defense Infrastructure (JEDI), let alone the ability to operate in heavily regulated industries such as healthcare and finance. It makes sense that CSPs would invest heavily in becoming world-class security experts.

Following the model of shared responsibility, customers are still responsible for any security controls they can touch. The CSP covers the physical security of their data centers, governance of their employees, infrastructure security of their servers and any of the “black boxes” or underlying software for their web services. Customers are responsible for all the rest: customer data, access control, firewall configuration and encryption, to name the biggest.

While CSPs have created new services to help meet all those demands, customers still struggle to configure and maintain them correctly. Even a perceived security shortcoming (despite whether they are legally accountable) could dampen a CSP’s reputation. They still have considerable incentive to help educate customers and simplify the process.



Customers

Responsability for Security “In” The Cloud

Customer Data

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-Side Data Encryption & Data Integryty Authentication

Server-Side Encryption (File System and/or Data)

Networking Traffic Protection (Encryption, Integrity, Identity)

AWS

Responsability for Security “Of” The Cloud

Software

Compute

Storage

Database

Networking

Hardware / AWS Global / Infrastructure

Regions

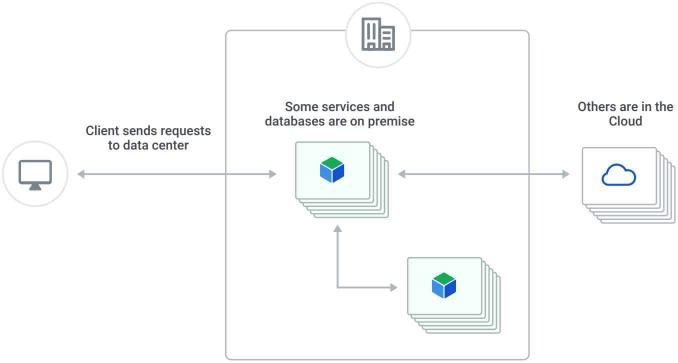
Availability Zones

Edge Locations

Source: https://aws.amazon.com/compliance/shared-responsibility-model/

For example, AWS believes its cloud native applications are the future and so has a cloud-native perspective on security. [1] Since the vast majority of enterprises do not run exclusively on the Cloud nor any single cloud, the concerns of shared responsibility multiply.

## Hybrid Cloud


Client sends requests to data center
Some services and databases are on premise
Others are in the Cloud

According to Gartner, more than 90 percent of companies will adopt a hybrid cloud model by 2020. [2] Companies that maintain a hybrid environment still need to worry about traditional data center issues such as physical security, server infrastructure and personnel with access to the facility.

Having a CSP offset some of their security concerns can still save millions of dollars, but there is increasing complexity. Many of a CSP's native security tools may not be compatible with those that are on-premise. The policy configurations may be awkward or difficult to apply universally. Even if a company accounts for cost savings and performance, security massively benefits from the ability to automate and standardize practices.

It becomes crucial for companies moving to the Cloud to be able to integrate existing tools, such as LDAP-based directory services. They need to be able to replicate controls across different contexts and for key and identity management to work from a single system of record. Especially concerning sensitive data such as personal health information (PHI), even if the Cloud is perfectly secure, they need to consider risks related to governance and compliance.

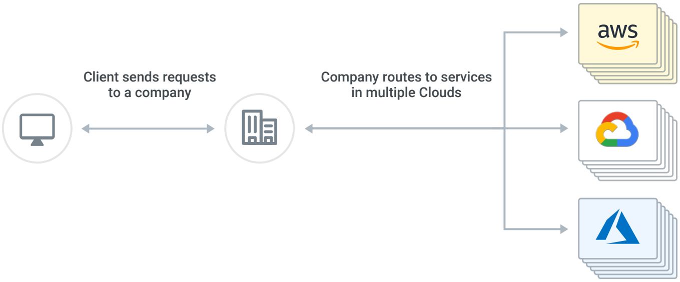
Availability and fault tolerance are age-old security concerns, as discussed in Part 1. The Cloud offers heavily automated ways to scale and a clear conceptual model to divide groups of infrastructure across geographical areas. All of these measures were to offset the reality that companies still face with data centers.

Hybrid-based companies still have the task of provisioning backup sites, constantly migrating data between physical locations and maintaining routines for different disaster recovery scenarios. Ensuring high availability in the face of security concerns such as DDoS attacks becomes far more complicated once one foot is off the Cloud.

## Multi-Cloud

It may seem far less of a risk to divide a workload across multiple clouds or at least to be able to quickly deploy a workload regardless of which cloud you happen to use. All of these scenarios illustrate why multi-cloud is attractive solely based on mitigating risk. [3]

The reality is that companies often just “end up” with multiple clouds rather than making a deliberate decision to divide their workloads accordingly. The ad hoc nature of this situation implies that a unified security model is an afterthought, even if the teams and departments deploying in each cloud are using strong security practices.


Client sends requests to a company
Company routes to services in multiple Clouds
aws

As described earlier, CSPs have an incredible economic incentive to protect their customers. That incentive only extends to customers in their own cloud or at least using a hybrid approach, but the incentive does not extend to multi-cloud. Even as CSPs recognize the reality of multi-cloud, it goes against their business models to easily enable movement to and from their competitors. As a result, it remains incredibly difficult to create a uniform set of policies that work with different types of native security tools.

# Part 3: Administrative Controls

## Policy as an Innovation

The most radical innovation of the last 500 years may not have been the internet or nuclear energy—but rather the rule of law. Until very recently, it was too dangerous to travel alone between cities. Now, a private citizen can traverse borders across the planet with little concern. The rule of law depends heavily on attribution, and here is where our challenge appears: it is notoriously difficult to attribute cyberattacks with absolute certainty. As a result, even enlightened legal systems that know better than to "blame the victim" will hold defenders accountable along with attackers. The result is that companies that would otherwise make otherwise rational choices are now heavily motivated by fear and heavy-handed requirements.

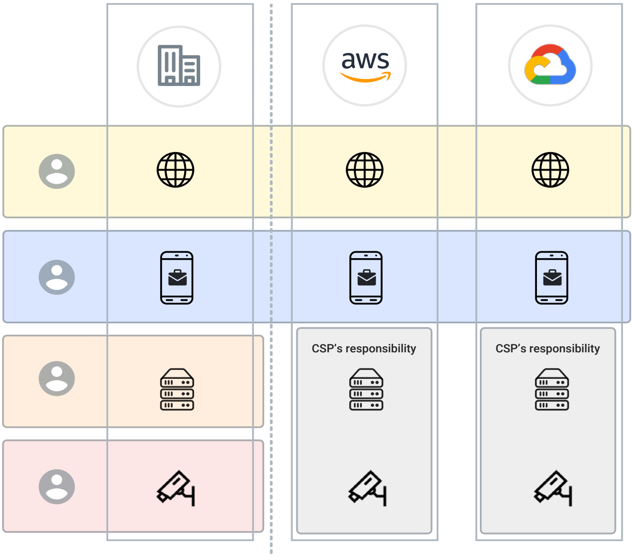
## Governance, Legal Issues and Compliance

The crux of cloud security is still the same as ever: the people make a real difference. While the Cloud has opened up the playing field to tiny companies and many different people across the world, the prevalence of laws, compliance and governance still linger. Those rules are often incredibly beneficial to the privacy and the safety of customers, so it would be a mistake to view them as a mere obstacle. Still, while they may introduce additional concerns that distract from what is truly necessary for security, they fall under the same purview.

As seen in Part 2's shared responsibility model, both a CSP and a company using them should be able to express their goals and establish a foundation for where and how they focus their security efforts. This model can be incredibly beneficial in communicating legal requirements and expectations while also making it less confusing to adhere to best practices. Since a company using the Cloud knows what a CSP is claiming responsibility for, the stakeholders responsible for legal decisions and risk mitigation can zero in on what they require from a CSP to trust them.

## Management Plane and Business Continuity

Multi-cloud offers a company to have freedom of choice when it comes to picking the best solution for each problem. It compels CSPs to be more competitive as a result. The variety of different environments does not come without its risks and cost: it requires more widely specialized personnel, more cross-system visibility and more leadership awareness for a variety of constantly evolving environments.



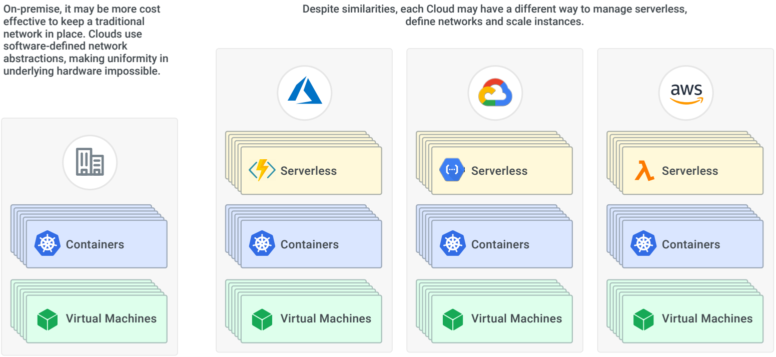
As a result, businesses may quickly encounter an issue with scaling and with business continuity based on how they manage (rather than merely who they hire). To maximize the benefits of the Cloud, much less hybrid or multi-cloud, companies need excellent managers to keep a handle both on evolving security controls and expanding compliance requirements for regulations. The best approach is to factor out the responsibility in two directions: accountability at the highest levels of an organization and motivation at all levels.

## Part 4: Technical Controls

### Infrastructure Security

With the advent of containers and serverless models, we stand at the forefront of redefining how software gets made. Still, the way it works at a logical level is fundamentally the same. Because it is the same, it does not always make sense for companies to migrate massive applications to serverless or container-based deployments. Serverless, in particular, requires rewriting code and rethinking data flow. Concurrence, latency and composability could make older models more appealing. Strict software licenses may even rule out the use of containers. The result is a mixed infrastructure. Some parts of an application run on containers in the Cloud, others in virtual machines on-premise, and a small percentage may be serverless in a cloud's managed offering.

The newer the infrastructure, the easier it is to manage patches and updates. CSPs and infrastructure providers realize that maintenance is a significant pain point, regardless of a company's size. Still, in the context of hybrid and multi-cloud, the issue only compounds. Tool providers are only starting to account for how to provision virtual machines (VMs), containers and functions across these mixed environments. CSPs still cannot even determine whether software providers they partner with scan their containers. The solution is to pick tooling that developers can confidently attest to the security of and include security measures as part of choosing infrastructure.


On-premise, it may be more cost effective to keep a traditional network in place. Clouds use software-defined network abstractions, making uniformity in underlying hardware impossible.
Despite similarities, each Cloud may have a different way to manage serverless, define networks and scale instances.
aws
Serverless
Serverless
Serverless
Containers
Containers
Containers
Containers
Virtual Machines
Virtual Machines
Virtual Machines
Virtual Machines

Beyond detection and monitoring, visibility now includes an understanding of how tools work. Companies have less reason to trust a black box than open source software, which has led to more public sharing. Unfortunately, API keys that accidentally find their way into a codebase now have a much broader audience, which includes a legion of tireless bots scanning repositories at all times. The notion that an API key is as sensitive as an encryption key or code-signing key still hasn't settled. The solution is to make it effortless to keep credentials outside of code, such as using IAM (identity and access management) roles rather than keys to communicate between services. Again, the limitation is that while a particular CSP may have a solution that works well internally, we still lack a new standard to communicate between clouds or on-premise. While those who are knowledgeable and capable have grown comfortable working around this limitation, their comfort level doesn't alter the prevalence of careless key-sharing. It's cold comfort to businesses that need fool-proof solutions.

## Identity and Access Management

With the advent of federated trust solutions such as OpenID Connect, it is now incredibly easy for a company to offload authentication and authorization controls to a third-party. The benefit is that those third parties invest millions into researching and developing their solutions. In contrast, a company might have a handful of generalists who end up storing credentials in plaintext. This solution is excellent even for multi-cloud and hybrid deployments since they are completely agnostic.

The problem returns to "customer responsibility"—who it assigns accounts to, how those people manage their credentials and the degree of permissions they have. As described in Part 3, a successful strategy, even within the latest cloud environments, relies on people feeling a shared sense of motivation, regardless of how companies and CSPs divide accountability. Whereas a company has a relatively straightforward technical path to adopting federated trust or directory services, the administrative piece can prove daunting.

Companies need to find a way to automate or greatly simplify several classic administrative controls. These include the principle of least privilege and the ability to update permissions rapidly based on organizational changes. These controls also include the ability to immediately terminate all access to the on-premise and cloud network if an employee separates. All of these considerations need to be in place when companies decide to add or remove a cloud or move certain types of data from one environment to another.

## Data Protection

At every point in the network, CSPs offer customers a way to use cryptographic protocols. Endpoint authentication, reliable VPNs (virtual private networks) and proxy servers support the confidentiality and integrity that these protocols offer. More nuanced approaches, such as mutual TLS (transport layer security), give a high degree of confidence that the entire line of communication (rather than just one point) is genuine and protected.

## Part 5: Unified Strategy

With the builder’s mentality, we can now see how every seemingly innocuous decision contains a trace of security. Like an architect in the Middle Ages, we should place every door, every wall and every road with absolute certainty that an attack is imminent. Security and operational consistency are never tradeoffs, so the talent doesn’t rest in being decisive about whether to implement them. Our skills rest in figuring out how to manage performance, cost optimization and resilience without ever compromising security.

As builders, we must have both poise and a sense of urgency in the face of this modern challenge. Entire industries find themselves stunned and perplexed. The means to their growth—of simplifying growth—have also opened new threats to business continuity. We can’t just invent more rules to solve this problem. Security issues start and end with human beings, but we won’t solve them by corporate fiat. The opportunity for innovation is to find a way to extend visibility and consistency across the expanse of our constellation: private data center or public cloud, open source or black box, and type 1 hypervisor or serverless.

# References

[1] https://konghq.com/wp-content/uploads/2019/04/01-Kong-Cloud-Native-FINAL.pdf

[2] https://techbeacon.com/security/4-hybrid-cloud-security-challenges-how-overcome-them

[3] Mohammed A. AlZain, Eric Pardede, Ben Soh, 2012 ““Cloud Computing Security: From Single to Multi-clouds”” 45th Hawaii International Conference on System Sciences, IEEE, pp: 7/12. Available at https:// ieeexplore.ieee.org/abstract/document/6149560

Konghq.com

**Kong Inc.**
contact@konghq.com

150 Spear Street, Suite 1600
San Francisco, CA 94105
USA