Microsoft Azure

CHECK POINT™


# INTRODUCTION TO
# CLOUD SECURITY BLUEPRINT 2.0

# Contents

# Introduction

As we learned from the Rightscale 2019 State of the Cloud Report from Flexera, cloud computing adoption is close to universal across organizations of all sizes: 94% of survey respondents reported that their organization uses the public cloud. We also see that enterprises continue to embrace hybrid and multi-cloud strategies (see Figure 1). Hybrid cloud adoption has grown from 51% to 58%, and multi-cloud adoption increased from 81% to 84% over the previous year.

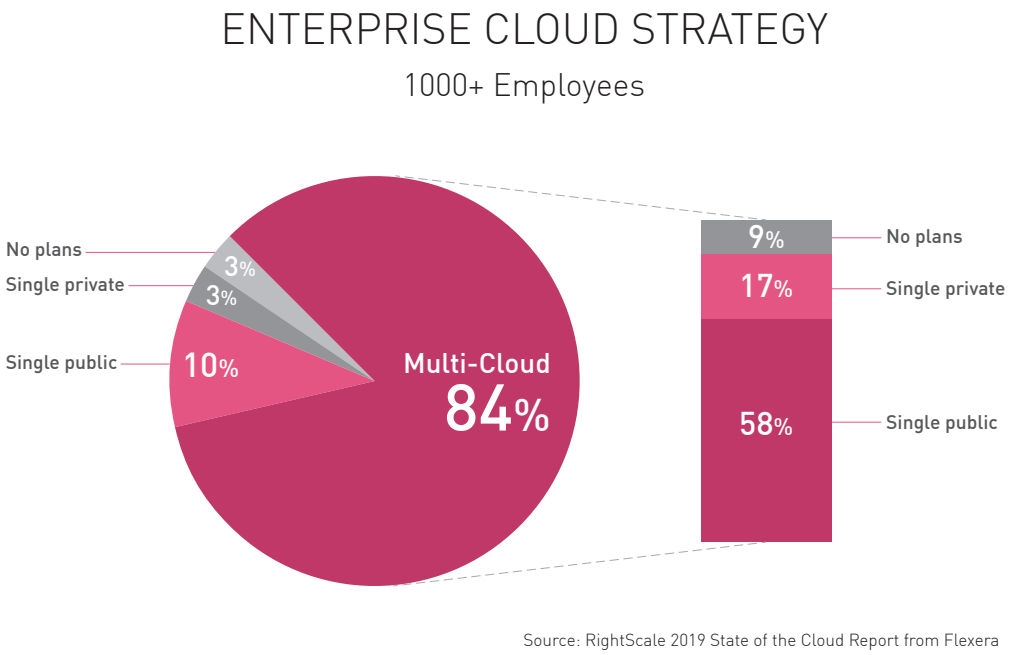


**Figure 1: Growth of enterprise hybrid and multi-cloud infrastructures**

Business agility, productivity, operational efficiency, flexibility, and profitability are undoubtedly the key drivers behind enterprise public cloud adoption. The public cloud allows compute-store-network resources to be acquired and deployed more rapidly. Once deployed, these resources can be scaled up or down as needed to meet demand.

Microsoft Azure

CHECK POINT

Research shows that as many as 10,000 businesses are vulnerable due to a widespread setting misconfiguration in Google Groups.

At the same time, however, Gartner's Security of the Cloud Primer for 2019 states that cloud security remains a top concern. This is not surprising when we consider that public cloud services are shared, always connected, and dynamic by nature. Furthermore, Gartner has predicted that "through 2022, 95% of cloud security failures will be the customer's fault." In fact, the majority of cloud breaches can be traced back to simple human errors rather than concerted attacks. For example, research shows that as many as 10,000 businesses are vulnerable due to a widespread setting misconfiguration in Google Groups. On one hand, these are alarming statistics. However, they also imply that enterprises can significantly improve their security posture if they deploy an effective security strategy.

Last year we published the Check Point Secure Cloud Blueprint v1.0 in order to help enterprises design and implement agile cloud security architectures. Because there have been a number of important changes to the cloud blueprint since then, we have chosen to publish a new series of white papers covering:

- An introduction to fundamental principles of the Cloud Blueprint
- How to enable Cloud Blueprint solutions
- Technical Cloud Blueprint implementation guidelines for leading cloud service providers

In this first white paper, we describe the key cloud security concepts and architectural principles that must underlie a cloud security blueprint.

# Cloud Security Concepts: A Primer

In this section, we review two key concepts an enterprise must understand in order to adopt an effective security blueprint.

## UNDERSTANDING THE SHARED RESPONSIBILITY MODEL OF THE PUBLIC CLOUD

Moving workloads and data to a public cloud environment means that security responsibilities are shared between you and your cloud provider. The security of the cloud infrastructure (including the actual physical data center locations, compute/network/storage hardware such as routers, switches, and load balancers, HVAC, electricity and so on) is delivered by the provider. It is the customer's responsibility to use the cloud provider's native tools to protect the assets and workloads it runs in the cloud including application code, application data, and application access—all while maintaining compliance with regulatory requirements and security best practices.

By definition, the shared responsibility model varies when using IaaS, PaaS, or SaaS services (see Figure 2, based on a diagram from the Microsoft Azure website). At the same time, most typical cloud implementations use a mix of these service models, which is often the cause of a common confusion: Who is responsible for what?

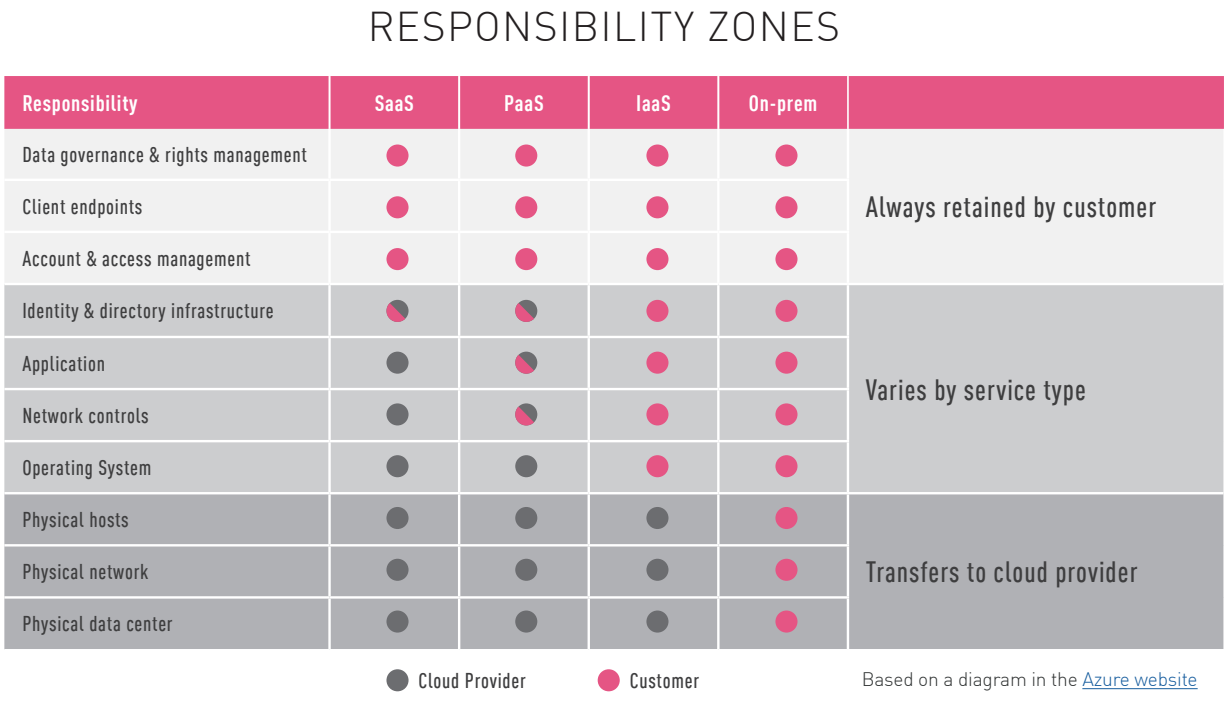


**Figure 2: Shared responsibility zones across cloud service models**

Microsoft Azure sums it up on their website:

> "...In an on-premises datacenter, you own the whole stack. As you move to the cloud some responsibilities transfer to Microsoft. For all cloud deployment types, you own your data and identities. You are responsible for protecting the security of your data and identities, on-premises resources, and the cloud components you control (which varies by service type).
>
> Regardless of the type of deployment, the following responsibilities are always retained by you:
>
> - Data
> - Endpoints
> - Account
> - Access Management

In short, cloud customers should not be lulled into complacency with the belief that "the cloud is secure." In fact, the security responsibility of cloud customers is significant and should never be taken lightly.

## ZERO TRUST AND WHY YOU SHOULD EMBRACE IT

Forrester states in its Predictions 2019 report, Transformation goes pragmatic, that "in 2019 and into 2020, Zero Trust will become the ad hoc standard in the US."

As its name implies, the basic principle of Zero Trust is not to trust anyone or anything—and verify everything. There are attackers both within and outside of the network and, by default, users and machines should never be automatically trusted. You need to assume that all traffic, regardless of location, is threat traffic until it is verified (i.e., authorized, inspected, and secured).

Zero Trust, for example, promotes a least privilege governance strategy whereby users are only given access to the resources they need to perform their duties. Furthermore, today's modern applications often grant extensive privileges to the components that comprise the distributed architecture. Web-facing applications are particularly vulnerable. For example, if the developer has not blocked ports consistently or has not implemented permissions on an "as needed" basis, a hacker who takes over the application will have privileges to retrieve and modify data from the database.

In addition, Zero Trust networks utilize micro-segmentation—a method of creating secure zones in data centers and cloud deployments that segments workloads from each other, secures everything inside the zone, and applies policies to secure traffic between zones. This makes network security far more granular. It is also important to continuously inspect and log all internal and external traffic in order to monitor for malicious activity with real-time protection capabilities.

The Forrester report cited above clearly states that we need to be:

> "building secure micro-perimeters, using obfuscation to increase data security, curbing excessive user privileges to limit risk, and employing automation and analytics to improve security detection and response. **The idea of a trusted internal network and an untrusted external network needs to be discarded** [our emphasis]. It demands that security teams verify and secure all resources regardless of location; limit and strictly enforce access control for all users, devices, channels, and hosting models; and log and inspect all internal and external traffic."

In all these ways and more, Zero Trust promotes security that is pervasive and proactive throughout the network, not only at the perimeter. Applying Zero Trust principles effectively minimizes the network's attack surface as well as the blast radius if and when an attack takes place.

It is also important to continuously inspect and log all internal and external traffic in order to monitor for malicious activity with real-time protection capabilities.

# Advanced Cloud Security Challenges

Because the public cloud does not have clear perimeters or egress/ingress ports, an organization that migrates to the cloud enters a fundamentally different security reality. This new security reality becomes even more challenging when adopting modern cloud approaches such as automated CI/CD methods, distributed serverless architectures, and ephemeral assets like Functions as a Service (FaaS) and containers.

In this section we discuss the advanced security challenges and the multiple layers of risk faced by today's cloud-oriented organizations.

## INCREASED ATTACK SURFACE

Malware, Zero-Day, Account Takeover and many other malicious threats have become a day-to-day reality. The public cloud environment has become a large and highly attractive attack surface for hackers who seek to exploit poorly secured cloud ingress ports in order to access and disrupt workloads and data in the cloud. Every organization that embraces the public cloud must understand that it significantly increases its attack surface just by using it.

## LACK OF VISIBILITY AND TRACKING

In general, companies have less visibility into cloud infrastructures than into on-premises infrastructures. In the IaaS model, the cloud providers have full control over the infrastructure layer and do not expose it to their customers. The lack of visibility and control is further extended in the PaaS and SaaS cloud models.

More specifically, cloud assets often become invisible and difficult to manage, which creates serious security enforcement gaps. Without next-generation orchestration tools, cloud customers cannot effectively identify and quantify their cloud assets or visualize their cloud environments.

## EVER-CHANGING WORKLOADS

Cloud assets are provisioned and decommissioned dynamically—at scale and at velocity. Traditional security tools are simply incapable of enforcing protection policies in such a flexible and dynamic environment. New tools and approaches are required to secure today's ever-changing and ephemeral workloads.

## DEVOPS, DEVSECOPS AND AUTOMATION

Organizations that have embraced the highly automated DevOps culture of Continuous Integration and Continuous Deployment (CI/CD) must ensure that appropriate security controls are identified and embedded

in code and templates early in the development cycle. Security-related changes implemented after a workload has been deployed in production can undermine the organization's security posture as well as lengthen time to market.

## GRANULAR PRIVILEGE AND KEY MANAGEMENT

It is not unusual for cloud user roles to be configured very loosely, granting extensive privileges beyond what is intended or required. One common example is giving database delete or write permissions to users who are untrained or simply have no business need to delete or add assets.

The situation is similar at the application level, where improperly configured keys and privileges create security risks through key leakage or poorly protected sessions.

In order to uphold the Zero Trust principle, user and application privileges must be managed at a highly granular level by flexible and dynamic permission management access tools.

## MULTI-CLOUD ENVIRONMENT

Each cloud provider offers tools and services to help its customers monitor and secure their cloud resources. It is good practice to integrate these cloud provider tools into your existing security stack in order to help fulfill your part in the shared responsibility model.

It is important to remember, however, that each provider's security tooling applies only to its own cloud services. In order to manage security in a consistent way in the hybrid and multi-cloud environments favored by enterprises these days, the organization needs configuration management, automatic remediation, and orchestration tools that work seamlessly across public cloud providers, private cloud providers, and on-premise deployments.

## COMPLIANCE AND REGULATIONS

Compliance with relevant laws or industry-specific regulatory requirements must be taken into consideration when operating in the cloud. In order to address their part of the shared responsibility model as it relates to compliance, all the leading cloud providers have aligned themselves with most of the well-known accreditation programs such as PCI 3.2, NIST 800-53, HIPAA, and GDPR. However, customers are responsible for ensuring that their workload and data processes are compliant.

In addition, given the poor visibility and dynamics of the cloud environment, the compliance audit process can be painstaking unless customers use tools that perform real-time and continuous compliance checks for misconfigurations, including alerting and automatic remediation as required.

# Cloud Security Architectural Principles

In this section, we look at the architectural principles that must be addressed by any enterprise-grade cloud deployment if it is going to meet the challenges of limited visibility, the need for granular authorization and privilege management, smooth integration with CI/CD automated processes, consistency across complex infrastructures, and upholding compliance requirements.

## NETWORK PERIMETER SECURITY WITH ADVANCED THREAT PROTECTION

In recent years, there has been a clear rise in both attack frequency and the sophistication of these attacks. The cloud extends an organization's attack surface and, in general, creates new security challenges in terms of how we carry out vulnerability scanning and protect web applications.

As noted above (see Understanding the Shared Responsibility Model), in the IaaS service model, the provider is responsible for security "of" the cloud, while the customer must take ownership of securing what's "in" the cloud. This makes the customer responsible for implementing best-in-class advanced threat protection and prevention at the network perimeter (i.e., the main junctions through which traffic enters and exits resources in the cloud environment), as per the shared responsibility model.

# OTHER ATTACK VECTORS TO BE SECURED

Other attack vectors that cloud security designs must address are:

| | |
|---|---|
| DATA | Data at rest must be secured on cloud storage resources such as Amazon S3, Microsoft Azure Storage, and Google Cloud Storage Bucket. Data in motion should be encrypted using tooling such as the Amazon EFS mount helper, Microsoft Azure client-side or server-side encryption, and GCP encryption in transit. |
| COMPUTE | In addition to standard virtual machines, a cloud security architecture must take into account today's highly distributed and dynamic application architectures that are based predominantly on serverless architectures, microservices, Functions as a Service (FaaS), Infrastructure as Code (IaC), and so on. The design should also provide protection for the advanced cloud PaaS products that support these architectures and services, including AWS Lambda, Microsoft Azure Functions, Google Cloud Functions, Amazon API Gateway, Amazon Elastic Container Registry and Microsoft Azure API Management. |
| MESSAGING | Similarly, modern web applications often use event-triggered messages to communicate among their highly distributed components. Perimeter protection must be implemented for managed messaging services such as Google Cloud's Cloud Pub/Sub, Microsoft's Azure Service Bus, and Amazon Simple Notification Service (SNS). |
| IDENTITY | Identity in cloud environments is comprised of access to the cloud environment (e.g., provisioning a new machine), as well as access to each specific resource (e.g., RDP access to this new machine). These are often completely separate and different. It is up to customers to identify and authorize users seeking to access their public cloud resources. Control plane protection must be implemented for the providers' access control services, such as AWS Identity and Access Management (IAM) and Microsoft Azure Active Directory. In addition, the customer must utilize Security Groups to dynamically control the access that logged-on users have to resources in the cloud. |

## SECURITY BY DESIGN

Misconfigurations are one of the primary root causes of data breaches in the cloud. Security by design means that the cloud security architecture should, wherever possible, leverage cloud infrastructure design characteristics in order to achieve immutable security (i.e., security that cannot be compromised by policy misconfigurations or bypasses). For example, there might be a requirement that a certain cloud data repository is never exposed to the internet. Rather than a firewall configuration, the preferable security-by-design best practice would be to never have any connection between the repository and an internet-facing hub.

This security-by-design approach is yet another example of how Zero Trust can and should be embraced in order to effectively protect cloud assets.

## SEGMENTATION AND MICRO-SEGMENTATION

A recent Proofpoint study of more than 100,000 unauthorized logins across millions of monitored cloud user accounts reveals that one in every three breaches involved a lateral movement between two or more points within the network. After breaching the network perimeter the attacker was able to infect other machines within that network. This behavior reinforces the need to implement the fundamental principle of the Zero Trust model, which is to further segment the network by application or service and place best in-class protection between those segments so that an attacker cannot move freely.

In order to implement segmentation as part of the Zero Trust model, and also to allow applications to securely communicate with each other, the security for each network segment is enforced at two security control points:

1. At the access level, a firewall is configured to allow whitelisted traffic to flow so that apps can operate normally, while at the same time, blocking unwanted traffic.

2. Traffic allowed at the access level is then thoroughly inspected (also known as Deep Packet Inspection) to identify and block malicious behavior on the application/data layer.

An organization's cloud security architecture must promote the automation of processes and tasks from the ground up.

## AGILITY

The on-demand, elasticity and scale characteristics of a public cloud let you operate and deploy workloads for your business at a higher velocity and with greater agility. Modern, efficient business practices are not possible if it takes weeks to provision servers and services or if security workflows are tedious and time-consuming.

Your cloud security architecture must cultivate and embrace agility while ensuring that speed does not contribute to loss of control or business risk. This principle is upheld by creating a scoped delegation of ownership among the different stakeholders in the organization, which gives DevOps, application owners, and others enhanced levels of authority over their resources and environments. Using Infrastructure as Code and other methods, DevOps teams can dynamically and programmatically implement access-control protection within and between their own workloads, while leaving perimeter protection and advanced security considerations to the Network and Security teams.

## AUTOMATION, EFFICIENCY, ELASTICITY

Cloud automation is a broad term that refers to the processes and tools an organization uses to reduce the manual efforts associated with provisioning and managing cloud resources. This is in stark contrast to legacy security approaches that rely heavily on manual protection of workloads and resources. If business agility is being constrained by security bottlenecks, these approaches will either be bypassed by workarounds or just opened up wide enough to not interfere, both of which can expose the organization to greater risk.

Reducing the human factor in cloud security operations through automation and programmatic operations not only supports business agility and operational efficiency, but also mitigates the risk of human error (i.e., misconfiguration), which is a very significant factor in security breaches. An organization's cloud security architecture must promote the automation of processes and tasks from the ground up. This starts at the environment provisioning phase (by using pre-configured templates, for example) and continues with day-to-day operations like using dynamic, adaptive security policies that do not require human intervention.

## BORDERLESS

It is becoming common practice for enterprise customers to embrace a multi-cloud strategy (i.e., the use of multiple cloud-computing providers in a single and heterogeneous environment). Although this strategy has many benefits, using a plethora of new and emerging technologies across multiple cloud providers over different geographic locations brings with it several security challenges, including:

- Enforcing a consistent security policy across all environments.
- Establishing unified and centralized management of the organization's security posture (i.e., identify, troubleshoot and resolve security incidents from one place).
- Securely interconnecting diverse cloud environments across multiple locations.
- Allowing applications to easily and securely communicate with each other regardless of their locations.
- Gaining visibility into the traffic flows within and between locations.

Thus, an effective cloud security architecture must be cloud-platform agnostic. The architecture should support a unified policy across public/private and on-premises environments, allowing security teams to focus on security, rather than on the mechanics of switching contexts among provider-specific security tools and services.

## COMPLIANCE

As discussed above in Compliance and Regulations, the cloud presents significant compliance and compliance audit challenges. An organization's cloud security architecture must ensure that workloads and data are compliant and that audits can be conducted seamlessly even across complex multi-cloud and hybrid infrastructures.

# Summary

The drivers for cloud adoption are usually agility, shorter time to market and the ability to innovate faster. The challenge for CISOs is how to support the business needs for cloud adoption and transformation without compromising on security or speed.

In this white paper we explain why customers must rethink their cloud security strategy and implement cloud security architectures that achieve:

- More flexible and agile security solutions
- All the business benefits of operating in the cloud but in a secure manner
- Advanced and comprehensive threat protection

However, as companies migrate modern and traditional workloads to the public cloud, it is important that they understand their role in the cloud providers' shared responsibility models. In the IaaS service model, for example, the provider is responsible for securing the infrastructure itself, but customers must take ownership of securing their own data, applications, and workloads. This task is even more complex when adding other cloud-native services, like PaaS and SaaS.

The tools offered by cloud providers to help customers implement secure cloud deployments are often inadequate in the face of today's advanced threats. It is also difficult to manage multi-cloud and hybrid environments using a fragmented stack comprised of provider-specific tooling.

Given the sophistication and scope of today's threat landscape, cloud security must embrace a Zero-Trust approach, in which users or machines are not automatically trusted. Users should be given only the minimum privileges, meaning those that they actually need to carry out their tasks. All traffic must be verified, and attack surfaces need to be minimized through effective network segmentation. Micro-segmentation of software-defined networks and distributed app architectures further enhances security postures.

These key principles should underlie any cloud security architecture:

- Advanced security for networks, as well as data, compute, messaging, and identity attack vectors.
- Systematic separation of all traffic flows (to, from, and within cloud environments).
- Segmentation by application or service and micro-segmentation of hosts running within the same segment or remotely.
- Cultivating agility for DevOps and lines of business without compromising the corporate security posture.
- Automation, efficiency, and elasticity in order to keep up with the velocity of business, while reducing risky human errors and misconfigurations by embedding security into code.
- A platform-agnostic, borderless architecture in which security policies can be enforced consistently across all environments.

For a discussion of the Blueprint 2.0 implementation model and practical solutions, see here.

To trial or purchase cloud security solutions on Azure Marketplace, see here for cloud network security and here for Cloud Security Posture Management.

**Worldwide Headquarters**
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

**U.S. Headquarters**
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

**www.checkpoint.com**