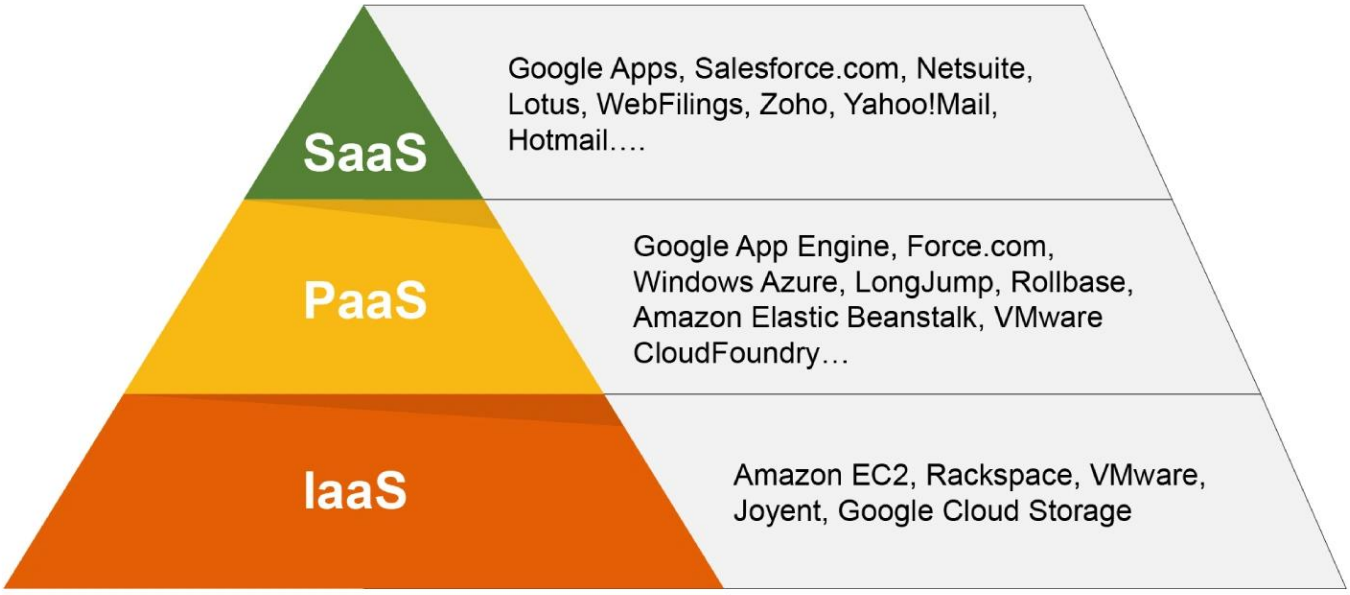
Understanding Shared Responsibility Model in Cloud Environment

Cloud service providers adhere to a shared security responsibility model, which includes ensuring physical security of their data centers and infrastructure, while your security team maintains some responsibilities for security as you move applications, data, containers, and workloads to the cloud. Defining the line between your responsibilities and those of your providers is imperative for reducing the risk of introducing vulnerabilities into your public, hybrid, and multi-cloud environments.

Shared Responsibility Varies by Provider and Service Type

In a traditional data centre model, you are responsible for security across your entire operating environment, including your applications, physical servers, user controls, and even physical security of the building. In a cloud environment, your provider offers valuable relief to your teams by taking on a share of many operational burdens, including security. In this shared responsibility model, security ownership must be clearly defined, with each party maintaining complete control over those assets, processes, and functions they own. By working together with your cloud provider and sharing portions of the security responsibilities, you can maintain a secure environment with less operational overhead.

Cloud Service Delivery Models and Shared Responsibility



Cloud service delivery models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), play a crucial role in determining the shared responsibility model. Each model delineates the division of security responsibilities between the cloud provider and the customer differently.

In an IaaS model, the cloud provider is responsible for the underlying infrastructure, which

includes the physical servers, networking, and data centres. The customer, on the other hand, is responsible for the operating system, applications, and data. This means that while the provider ensures the security of the physical infrastructure and virtualization layer, the customer must manage the security configuration of the operating system, applications, and data.

In a PaaS model, the provider takes on more responsibility by managing the underlying infrastructure and the platform itself. This includes the operating system and middleware. The customer is then responsible for the applications they deploy and the data they store. This model reduces the operational burden on the customer but still requires them to secure their applications and data.

In a SaaS model, the provider is responsible for the entire stack, including the application, platform, and infrastructure. The customer's responsibility is primarily focused on data security and user access management. This model offers the highest level of convenience but still requires the customer to ensure proper data handling and access controls.

Understanding the cloud service delivery model is essential for determining the shared responsibility model. Customers must carefully review the service level agreement (SLA) and understand the security responsibilities of both the provider and the customer. By doing so, customers can ensure that they are meeting their security obligations, and that the provider is meeting theirs.

Defining the lines in a shared responsibility model

The key to a successful security implementation in a cloud environment is understanding where your provider's responsibility ends, and where yours begins. The answer isn't always clear-cut, and definitions of the shared responsibility security model can vary between service providers and can change based on whether you are using infrastructure-as-a-service (IaaS) or platform-as-a-service (Paas):

- In the AWS Shared Security model, AWS claims responsibility for "protecting the hardware, software, networking, and facilities that run AWS Cloud services."
- Microsoft Azure claims security ownership of "physical hosts, networks, and data centers," ensuring physical security and operational integrity. Both AWS and Azure state that your retained security responsibilities depend upon which services you select.

While the wording is similar, shared responsibility agreements leave much open for discussion and interpretation. But there are always some aspects of security that are clearly owned by the provider and others that you will always retain. For the services, applications, and controls between those ownership layers, security responsibilities vary by cloud provider and service type. In a multi-cloud environment, these variations in ownership introduce complexity and risk. Each environment, application, and service requires a unique approach for security assessment and monitoring. However, your overall security posture is defined by your weakest link. If you have a gap in coverage in any one system, you increase vulnerability across the entire stack and out to any connected systems.

Navigating Cloud Security's Shared Responsibility Model

In this whitepaper you will discover:

- The Basics of Shared Responsibility Models
-

Security Automation Attributes

- Integrating with Fidelis Halo

Download Whitepaper

A vendor-agnostic look at shared responsibility

The following diagram provides a high-level, vendor-agnostic view of a shared responsibility model based on concepts, rather than service level agreements. This includes ensuring physical security of the data centers and infrastructure that support cloud services. When entering into a discussion with a cloud provider, security needs to be included upfront in the decision-making process regarding shared responsibilities. You can use this guide to inform your discussion and to understand your roles and responsibilities in securing your cloud implementation.

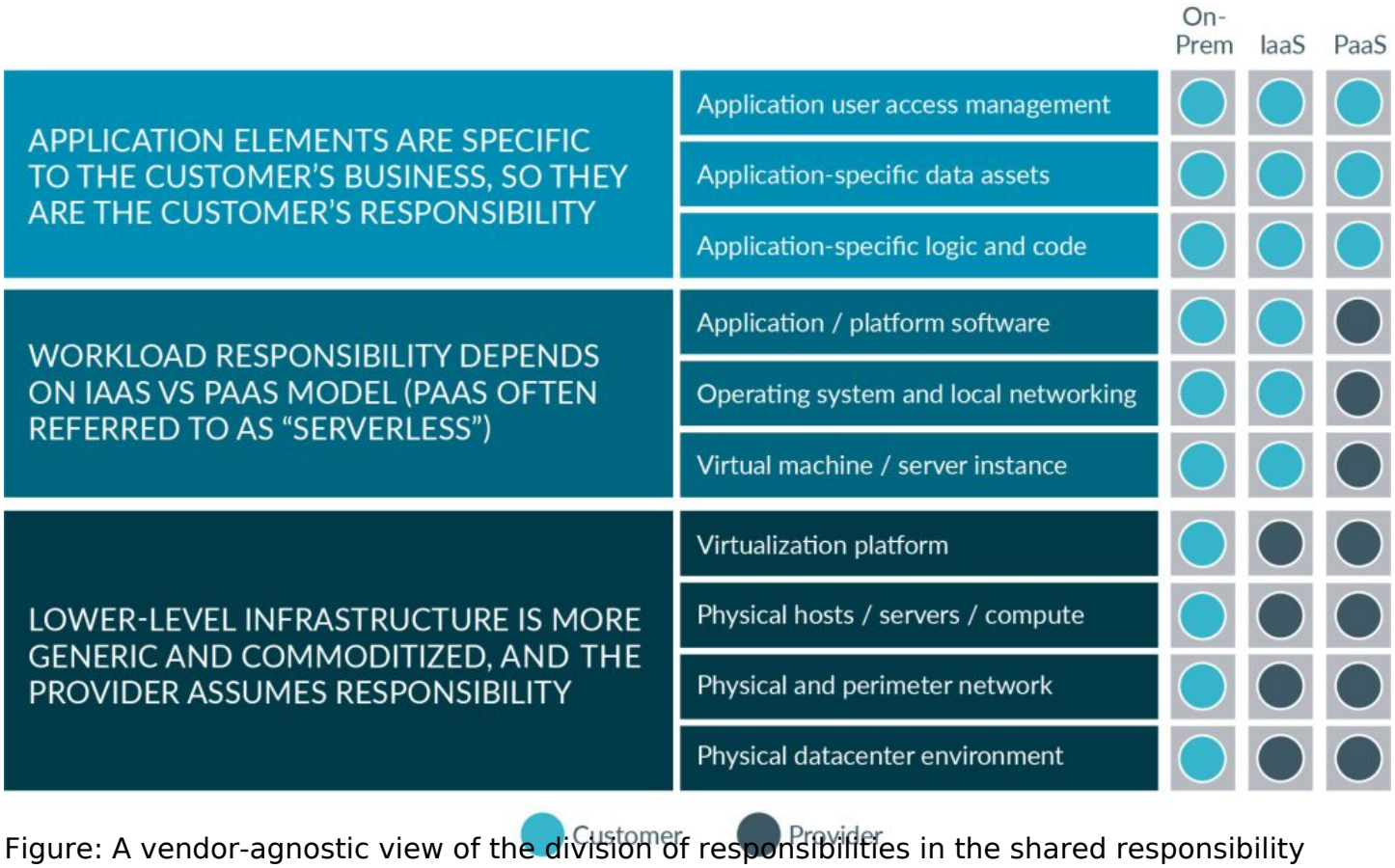


Figure: A vendor-agnostic view of the division of responsibilities in the shared responsibility model

Your Share of Cloud Security Responsibilities

Whether in the data center, or using a server-based IaaS instance, serverless systems, or a PaaS cloud service, you are always responsible for securing what's under your direct control, including:

- **Information:** By retaining control over information and data, you dictate the terms of their usage and timing. Your provider has zero visibility into your data, and all data access is yours to control by design.

- **Application Logic and Code:** Regardless of how you choose to spin up cloud resources,

your proprietary applications are yours to secure and control throughout the entire application lifecycle. This includes securing your code repositories from malicious misuse or intrusion, application build testing throughout the development and integration process, ensuring secure production access, and maintaining security of any connected systems.

- **Identity and Access:** You are responsible for all facets of your identity and access management (IAM), including authentication and authorization mechanisms, single sign-on (SSO), multi-factor authentication (MFA), access keys, certificates, user creation processes, and password management.

- **Platform and Resource Configuration:** When you spin up cloud environments, you control the operating environment. How you maintain control over those environments varies based on whether your instances are server based or serverless. A server-based instance requires more hands-on control over security, including OS and application hardening, maintaining OS and application patches, etc. In essence, your server-based instances in the cloud behave similar to your physical servers, and function as an extension of your datacenter. For serverless resources, your provider's control plane gives you access to the setup of your configuration, and you are responsible for knowing how to configure your instance in a secure manner.

Additionally, you maintain responsibility for securing everything in your organization that connects with the cloud, including your on-premises infrastructure stack and user devices, owned networks, and applications, and the communication layers that connect your users, both internal and external, to the cloud and to each other. You'll also need to set up your own monitoring and alerting for security threats, incidents, and responses for those domains that remain under your control. These responsibilities are yours whether you are running on AWS, Azure, or any other public cloud provider's systems.

Comprehensive CNAPP solution for Unified Cloud Security

Gain unmatched visibility across every cloud server and container with Fidelis Halo:

- Frictionless Operation
- Heartbeat Monitoring
- Comprehensive File Integrity Monitoring

Download Datasheet

Understanding the Gray Areas of the Shared Responsibility Model

Based on whether you are running an IaaS or PaaS implementation, you may retain additional security responsibilities, or your provider may take some of that burden off your team. The line between your responsibility and those of your cloud vendor is dependent upon selected services and the terms of those services.

In the case of server-based instances, you often assume full responsibility of:

- **Identity and Directory Infrastructure:** Whether you're using OS-level identity

directories like Microsoft Active Directory or LDAP on Linux, or you opt for a third-party identity directory solution, the security configuration and monitoring of that system is yours to control in an IaaS cloud implementation.

- **Applications:** Server-based cloud environments, much like on-premises hosts, are a blank slate for installing and maintaining applications and workloads. You may run PaaS applications on your cloud servers, in which case you might be relieved of some of the security burden. However, any application or workload you move from your data center to a server-based instance in the cloud is solely your responsibility to secure.

- **Network Controls:** Your provider only maintains the network that's directly under their control. All networking above the virtualization layer—whether physical or infrastructure-as-code—requires your security configuration and monitoring.

- **Operating System:** With server-based instances, you get to choose your OS and patch levels. While this allows you greater flexibility, it also means greater responsibility when it comes to security. You'll need to keep up with current vulnerabilities, security patches, and environment hardening exercises to keep your server-based cloud resources secured.

When you choose a serverless environment or PaaS solutions, you do alleviate some of the security burden. Serverless solutions provide a control plane for configuration, and you are responsible for configuring that service in a secure manner. For example, in a serverless environment, you may have the opportunity to choose an operating system (typically Microsoft or Linux), but your provider maintains responsibility of the OS patching and security management in that environment. Serverless environments typically provide some management of the physical implementation of your identity and directory infrastructure, applications, and network controls as well, but you are still responsible for properly configuring access management through the control plane.

Responsibilities Always Owned by Your Cloud Service Provider

While it may seem that you retain a significant share of security responsibilities, your provider does alleviate much of your burden. Cloud vendors maintain 100% of control over the security of:

- **The Virtualization Layer:** By controlling the provisioning of physical resources through virtualization, providers ensure segmentation and isolation of CPU, GPU, storage and memory to protect your users, applications, and data. This layer of abstraction acts as both a gateway and a fence, allowing access to provisioned resources, and protecting against potential misuse or malicious intrusion, both from the user environments, down, and the physical layer, up.

- **Physical Hosts, Network and Datacenter:** Cloud vendors protect their hardware through a variety of both software and physical security measures. Large cloud providers like AWS and Azure protect their servers from physical intrusion and tampering through a variety of protocols, and they also ensure rapid failover and high availability with comprehensive, built-in backup, restore, and disaster recovery solutions.

The Shared Responsibility Model in Practice

When speaking of "shared responsibility," it's important to understand that you and your cloud

provider never share responsibility for a single aspect of security operations. The areas of ownership you control are yours alone, and your provider does not dictate how you secure your systems. Likewise, you have no control over how the provider secures their portions of the application and infrastructure stack. You do, however, have the ability and right to access your cloud vendor's audit reports to verify that their systems are secure and that they are adhering to your terms of service. Cloud providers publish these reports regularly and freely, and the most current reports are accessible at all times.

How the shared responsibility model impacts your developers

Cloud services offer convenient, automated environment provisioning, allowing developers and test groups to spin up servers through self-service processes. These environments, however beneficial for innovative potential, are often connected to your production assets and can pose significant security risks if not properly configured. While the cloud is inherently secure from the provider's perspective, a secure cloud requires proper configuration and diligent access management. Gartner states the misconfiguration accounts for 99% of cloud security failures. For would-be hackers, cloud development and testing environments that are set up without enforcing proper security policies can become a gateway into your production systems or proprietary code storage. This means that identity and access management and environment configuration management must be closely managed, sometimes at the expense of unfettered convenience. Centralized, automated access management and policy-driven environment creation are critical for the success of your cloud security implementation.

Securing the DevOps pipeline

Cloud applications, powered by an automated CI/CD pipeline and driven by a DevOps organization, accelerate the speed at which your business delivers new applications and features. Unfortunately, that also means your DevOps pipeline can inadvertently and rapidly introduce security vulnerabilities without proper consideration and management. In a shared responsibility model, you are responsible for securing your code and the tools you use to deliver applications to the cloud. The servers and serverless assets that make up your DevOps toolchain must be protected, including code repositories, Docker image registries, Jenkins orchestration tools, etc. Beyond securing your CI/CD pipeline, you can—and should—leverage CI/CD automation processes to shift security left, by integrating security into the code and making it part of the build. This idea of "shifting left" means automated testing against clearly defined security requirements, early and often in the development process, so that new vulnerabilities are caught and remediated before being merged into the larger code tree or introduced into a production service.

Shared responsibility and configuration management

The speed and ease of configuring software-defined infrastructure opens your company up to new levels of agility and adaptability. However, the ability to reconfigure resources on the fly can also have instantaneous and broad-reaching consequences. The potential for misconfiguration can lead to security vulnerabilities. Your operations team needs to work closely with security to maintain policy-based control over how and when your cloud resources are provisioned. Your security teams are also accountable for monitoring resource management in the cloud for potential vulnerabilities. Through scripting, automation, and carefully planned self-service workflows, your configuration management and security teams can work together to give your company controlled, secure access to the cloud resources they need without becoming a bottleneck.

Compliance management, threat management, and visibility into the cloud

Regardless of where your security responsibilities end and your cloud provider's responsibilities start, compliance with your organizational standards and required regulatory boards is your company's responsibility. Centralized security orchestration, automation, and response allows you to collect and analyze data across your entire infrastructure, including your on-premises systems, public, hybrid and multi-cloud environments, and out to your edge and endpoints. With the right security platform in place, your teams gain deep visibility that allows you to analyze and respond to threats and maintain compliance, often without human involvement.

Cloud Security Best Practices

Ensuring the security of cloud environments requires adherence to a set of best practices. These practices help in maintaining a robust security posture and mitigating potential risks. Here are some essential cloud security best practices:

1. **Implement a Cloud Security Framework**: Establish a comprehensive security framework that clearly outlines the security responsibilities of both the provider and the customer. This framework should serve as a guide for all security-related activities and decisions.
2. **Conduct Regular Security Audits and Risk Assessments**: Regularly perform security audits and risk assessments to identify and address potential vulnerabilities. This proactive approach helps in maintaining a secure environment and mitigating risks before they can be exploited.
3. **Define and Understand Security Responsibilities**: Ensure that the security responsibilities are clearly defined and understood by both the provider and the customer. This clarity helps in avoiding any gaps in security coverage and ensures that all aspects of security are adequately addressed.
4. **Provide Security Training and Awareness**: Educate and train your team on their security obligations and best practices. Regular training sessions and awareness programs help in keeping everyone informed about the latest security threats and how to handle them.
5. **Implement Security Controls**: Deploy robust security controls such as firewalls, intrusion detection systems, and encryption to protect your cloud resources. These controls act as the first line of defense against potential security threats.
6. **Monitor Cloud Resources for Security Threats**: Continuously monitor your cloud resources for any signs of security threats or incidents. Implementing automated monitoring tools can help in quickly detecting and responding to potential security breaches.
7. **Ensure a Robust Incident Response Plan**: Work with your cloud provider to ensure that there is a robust incident response plan in place. This plan should outline the steps to be taken in the event of a security incident, ensuring a swift and effective response.

By following these best practices, customers can ensure that their cloud environments are secure and that they are meeting their security obligations. These practices not only help in protecting cloud resources but also in maintaining a strong security posture in the ever-evolving landscape of cloud security.

Shared Responsibility Model Next Steps

Any time your cloud provider takes on a portion of security responsibility, it becomes one less concern for your organization. Clearly defined shared responsibilities allow you to focus your

efforts on your application delivery strategy without overburdening your teams with day-to-day operational concerns in the physical layer. A security platform that unifies and automates security controls from the data center and across each cloud simplifies security management and minimizes risk. Centralized control and configuration of the provider control plane, hosting, and orchestration for containers, applications, and workloads further improves coverage of your environment from end to end.

Frequently Ask Questions

What is the shared responsibility model?

The shared responsibility model provides a working framework for cloud service providers to detail responsibility for an entire cloud environment, including the hardware, data, identity, workload, networks, networking, settings, etc.

What is the principle of shared responsibility?

This principle applies in the context of shared responsibility where global, locale or individual actors are assigned the same responsibility according to each function or capability defined by the Principle of optimal attribution of role or responsibility.