Unlocking Cloud Security

The Shared Responsibility Model

Strategic Framework for Digital Liability Management

99% of Cloud Security Failures Are Customer Responsibility—Not Provider Failures

Understanding Shared Responsibility Through a Simple Analogy

Landlord (CSP)

- Building structure and foundation
- Main plumbing and electrical
- Physical security
- Core utilities and infrastructure
- Building-wide safety systems

THE LINE

Tenant (You)

- Locking your front door
- Securing your possessions
- Managing who gets keys
- Configuring your apartment
- Protecting your data

The Clear Boundary: If the tenant leaves their door unlocked, the landlord is not liable for theft. **Responsibility is clearly defined, and accountability follows the boundary.**

The Formal Contract: Two Distinct Security Domains

Security "OF" the Cloud

Provider Responsibility

Physical Security

- Biometric access controls
- CCTV monitoring
- Redundant power supplies

Core Infrastructure

- Physical servers and storage
- Networking hardware
- Data center facilities

Virtualization Layer

- Host operating systems
- Hypervisor security
- Workload isolation

Security "IN" the Cloud

Customer Responsibility

Data Protection

- Data classification
- Encryption at rest
- Encryption in transit

Identity & Access Management

- User permissions management
- Multi-Factor Authentication (MFA)
- Least privilege principle

Application & Configuration

- Security group firewalls
- Network settings
- Operating system patches

Infrastructure as a Service: Maximum Control Means Maximum Responsibility

What is IaaS? Infrastructure as a Service provides fundamental computing building blocks—virtual servers, storage, and networking. The customer has maximum control and, therefore, maximum responsibility.

You Manage (Customer)

- → Guest operating systems and updates
- → Security patches and hotfixes
- → Applications and middleware
- → Data protection and encryption
- → Network configurations and firewalls
- → Identity and access management

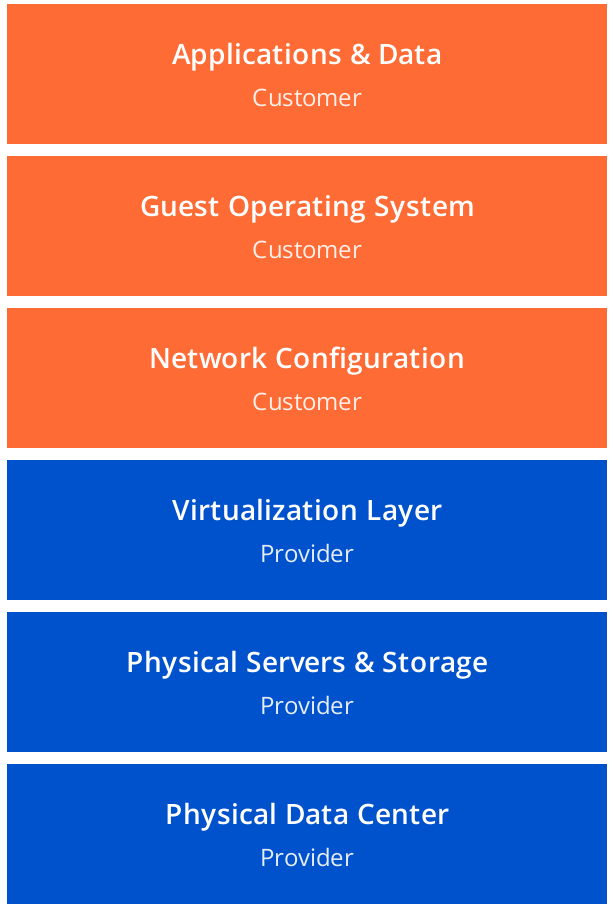
Provider Manages

- → Physical infrastructure and servers
- → Virtualization layer and hypervisors
- → Data center security and facilities
- → Hardware maintenance and updates

Next: Visual responsibility stack, apartment analogy, and risk profile assessment

IaaS: The Responsibility Stack

Visual representation of layered responsibilities



The Apartment Analogy

Renting an empty concrete shell of an apartment. The landlord provides the secure structure and utility hookups, but you are responsible for building out everything inside—walls, plumbing, electrical, and securing it all with your own locks.

Risk Profile

⚠ Highest customer responsibility; most misconfiguration opportunities. Your organization must invest heavily in security controls and configuration governance.

PaaS and SaaS: Shifting Responsibility

Platform as a Service (PaaS)

Provider Manages

- Hardware & servers
- Operating systems
- Runtime environment
- Platform maintenance
- Infrastructure security

You Manage

- Application code
- Data security
- User access control
- Data classification
- Encryption strategy

Analogy

Like renting a fully equipped workshop. The landlord provides the building, power, and maintains the heavy machinery (the platform), but you secure your own projects, tools, and materials (your code and data).

Software as a Service (SaaS)

Provider Manages

- Entire application stack
- Infrastructure & servers
- Application code
- Updates & patches
- System security

You Manage

- User access control
- Data security
- Data governance
- Sensitive data handling
- Compliance within app

Analogy

Like leasing a fully serviced office. The landlord manages the building, security, utilities, and furniture. Your responsibility is managing who gets keys to your office and securing sensitive documents you store inside.

Critical Insight: While provider responsibilities increase as you move from PaaS to SaaS, your accountability for data and user access management never changes. You always retain ultimate responsibility for securing what matters most to your organization.

You Can Share Responsibility, But You Cannot Share Accountability

What IS Shared

Security responsibilities are divided between provider and customer based on the service model and infrastructure architecture.

- ✓ Provider secures infrastructure
- ✓ Customer secures configuration
- ✓ Both contribute to overall security posture
- ✓ Clear boundaries defined by SRM

What Is NOT Shared

A single misconfiguration on your side results in **100% customer liability** for the resulting breach and all damages.

- ⚠ Weak Identity & Access Management
- ⚠ Unencrypted sensitive data
- ⚠ Misconfigured security groups
- ⚠ Unpatched systems and applications

100% Customer Liability

Financial penalties, regulatory fines, reputational damage, and customer trust loss fall entirely on your organization.

The Shared Responsibility Model Is Your Blueprint for Compliance

KEY REGULATORY FRAMEWORKS

- SOC 2
- HIPAA
- GDPR
- PCI-DSS

Provider Contribution

- ✓ Third-party audit reports (SOC 2)
- ✓ Infrastructure security attestation
- ✓ Compliance certifications
- ✓ Security control documentation

Customer Contribution

- ✓ Configuration logs and audit trails
- ✓ Access control reviews
- ✓ Security policy documentation
- ✓ Data protection evidence

Strategic Advantage: Clear responsibility division streamlines the audit process, ensures all compliance obligations are met by the responsible party, and demonstrates organizational control to auditors and regulators.

Evolution: From Shared Responsibility to Shared Fate

TRADITIONAL MODEL

- Clear division of duties
- Provider secures infrastructure
- Customer secures configuration
- Reactive approach

THE EVOLUTION

- Providers recognize customer challenges
- Increased collaboration
- Proactive support tools
- Shared success focus

SHARED FATE

- Mutual success orientation
- Provider invests in customer security
- Collaborative partnership
- Proactive resilience

Security-Hardened Templates

Infrastructure code templates and blueprints that allow customers to deploy workloads using security best practices enabled by default, reducing misconfiguration risk.

Opinionated Best Practices

Clear, transparent guidance on recommended security controls and settings, helping customers navigate the complexity of cloud security with expert recommendations.

Cyber-Insurance Programs

Innovative programs that help customers quantify, manage, and mitigate their residual risk, providing financial protection and risk management support.

By working together, providers and customers can close the gaps that lead to breaches and create an environment where innovation can thrive securely.

Five Critical Actions to Operationalize Cloud Security Accountability

1

Clarify Responsibility Boundaries

Map your cloud services to the Shared Responsibility Model. Document who owns what, ensuring no gaps exist between provider and customer responsibilities.

2

Invest in Identity & Access Management

Strong IAM is non-negotiable. Implement MFA, enforce least privilege, and conduct regular access reviews to prevent account takeovers and unauthorized access.

3

Implement Data Protection

Classify all data, encrypt at rest and in transit, and establish reliable backup and recovery procedures. Data security is your ultimate responsibility.

4

Establish Configuration Governance

Implement regular security audits, establish configuration baselines, and maintain patch management discipline. Misconfiguration is the leading cause of breaches.

5

Build a Security Partnership

Leverage provider tools, best practices, and security templates. Consider cyber-insurance programs to quantify and mitigate residual risk collaboratively.

Cloud security is a shared responsibility. Your organization's success depends on understanding and operationalizing this partnership.