

The top half of the image features a photograph of two people silhouetted against a vibrant sunset sky. One person is standing on a dark rock, leaning forward and reaching out to assist another person who is climbing up. The sun is low on the horizon, creating a warm, orange and yellow glow that fills the sky with soft, wispy clouds. The overall mood is one of teamwork and overcoming challenges.

Beyond the Shared Responsibility Model

Best Practices for Cloud Account and Workload
Visibility for the Hybrid Cloud



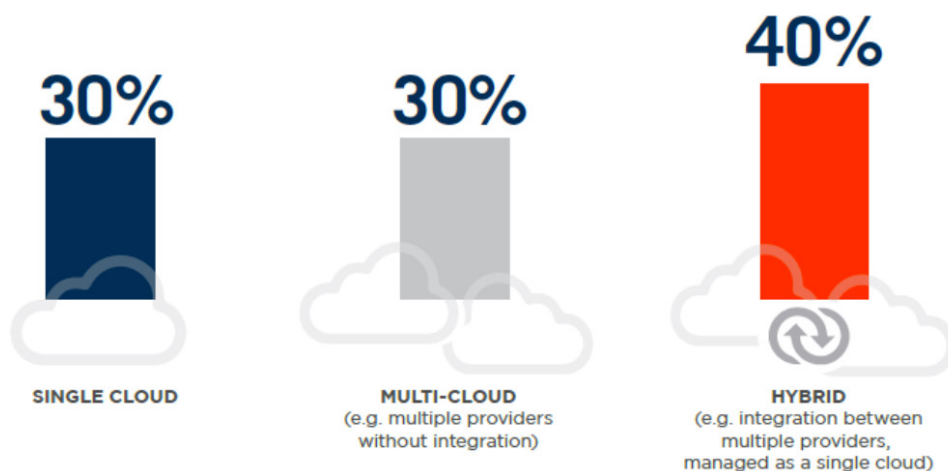
Responsibility Across the Hybrid Cloud

Many organizations now understand the shared responsibility model, with the major cloud providers going out of their way to educate their customers and prospects. But it is not as simple as just drawing a line and stating that the customer's role is 'above the line' and the provider's role is 'below the line.' It is different for SaaS, PaaS, and IaaS, and within each, the choice of provider-based services vs those offered by 3rd parties can seem confusing. And, understanding what exactly the different layers of the model entail many times takes an equal analysis of the specific service in question. Given that organizations are adopting a multi and hybrid cloud approach, the IT team must take into account the different services and monitoring interfaces across the different providers, and plan accordingly. Correlating data across multiple clouds, and introducing containers, yet adds another layer of complexity.

**Through 2020,
95% of cloud
security failures
will be the
customer's
fault.**

Gartner

► What is your primary cloud deployment strategy?



IaaS, PaaS, and SaaS Security

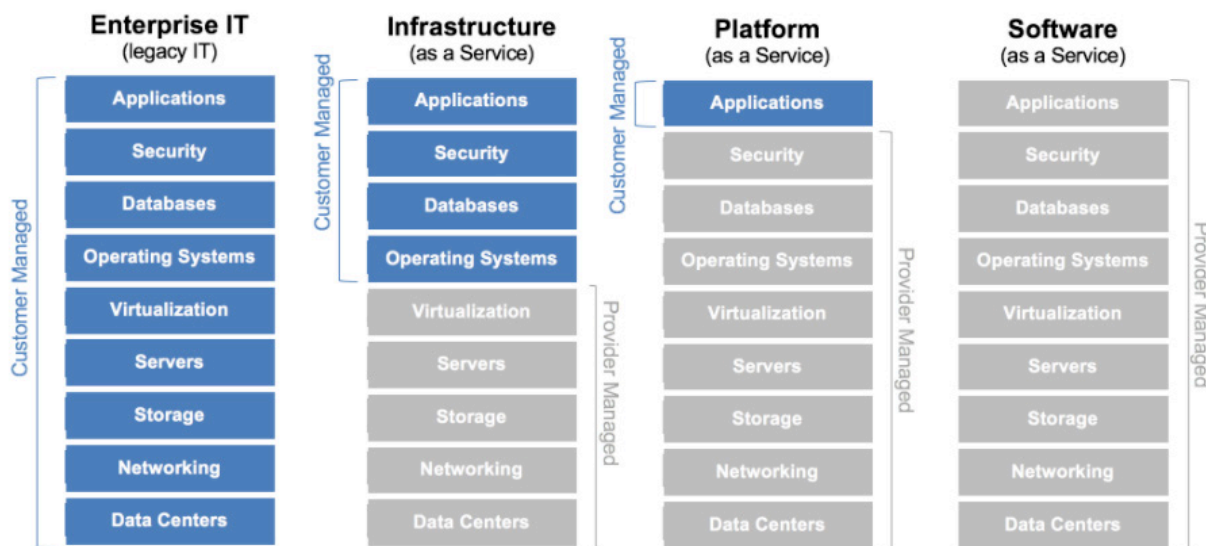
Within IaaS, the enterprise has the most control over their security posture, responsible for accreditation, certifications, and external audits. An organization on IaaS has the greatest responsibility for securing the bare-metal or virtualized OS, containers, as well as their applications and data.

Under a PaaS model, the enterprise relies on the cloud provider for OS security, responsible only for the applications and data, and must check that the CSP's services follow best practices.

Finally, within a SaaS deployment, the application is the service. Though the enterprise itself has less of a security role, SaaS, in general introduces additional concerns in that the enterprise needs assurance that the SaaS operator is following best practices. Within both PaaS and SaaS, the enterprise relies on their platform or software partners to carry out OS hardening and maintain compliance.

**By 2018, 60%
of enterprises
that implement
appropriate
cloud visibility
and control tools
will experience
one-third fewer
security failures.**

Gartner



2018 Cloud Security Report Findings

Produced by the Information Security Community on LinkedIn in partnership with Cybersecurity Insiders, this report highlights how organizations are responding to security threats in the cloud, and what tools and best practices IT cybersecurity leaders are considering in their move to the cloud. Some of the findings:

**01**

Cloud security concerns – While adoption of cloud computing continues to surge, security concerns are showing no signs of abating. Reversing a multi-year downward trend, nine out of ten cybersecurity professionals confirm they are concerned about cloud security, up 11 percentage points from last year's cloud security survey. The top three cloud security challenges include protecting against data loss and leakage (67 percent), threats to data privacy (61 percent), and breaches of confidentiality (53 percent).

**02**

Biggest threats to cloud security – Misconfiguration of cloud platforms jumped to the number one spot in this year's survey as the single biggest threat to cloud security (62 percent). This is followed by unauthorized access through misuse of employee credentials and improper access controls (55 percent), and insecure interfaces/APIs (50 percent).

**03**

Cloud security headaches – As more workloads move to the cloud, cybersecurity professionals are increasingly realizing the complications to protect these workloads. The top three security control challenges SOC's are struggling with are visibility into infrastructure security (43 percent), compliance (38 percent), and setting consistent security policies across cloud and on-premises environments (35 percent).

04

Legacy security tools limited in the cloud – Only 16 percent of organizations report that the capabilities of traditional security tools are sufficient to manage security across the cloud, a 6 percentage point drop from our previous survey. Eighty four percent say traditional security solutions either don't work at all in cloud environments or have only limited functionality.

05

Public cloud providers have continued to mature and expand their service offerings

– The two biggest cloud providers continue to compete for the lead in our survey: Amazon Web Services (72 percent) and Microsoft Azure (71 percent). Interestingly, Rackspace Cloud (67 percent) displaced Google Cloud Platform (54 percent) among our survey participants to claim third place this year.

06

Forty percent of organizations primary cloud deployment strategy is a hybrid cloud

– optimizing their investment by integrating multiple cloud providers to work together as a single, seamless environment. The remaining respondents equally said their cloud deployment of choice is either a single cloud (30 percent) or a non integrated, multi-cloud solution (30 percent).

IaaS Best Practices

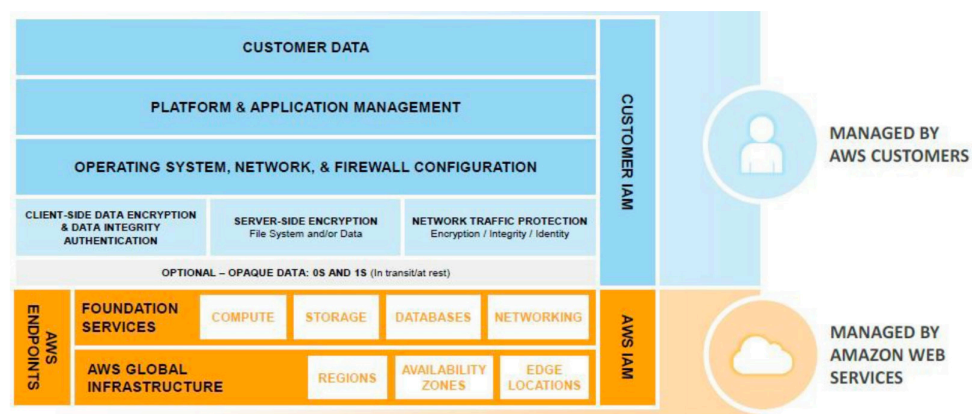
According to Gartner, the highest revenue growth in 2017 came from IaaS, which grew by over 35 percent. Here are some of the best IaaS practices when migrating to the cloud:

- Use a hardened OS image provided by AWS, CIS, or an off-the-shelf image then hardened via one of the CIS benchmarks.
- Automate the compliance of critical workloads running on the OS via a system that can conduct continuous assessments, against regulations such as PCI, SOC2, HIPAA, GDPR, and others. Mechanize patching and restrict access.
- Utilize the added layer of security provided by AWS CloudFormation templates for PCI and HIPAA.
- Confirm network and firewall configuration applying to the customer's AWS account and VPC(s).
- Ensure proper account, security group, and IAM management.
- Monitor the various AWS services utilized via CloudTrail, CloudWatch, Inspector, or GuardDuty.
- Set policies correctly based on applications and data, UEBA and implement least privilege.
- Implement data encryption, SLP, secure access, logging, and SIM/FIM

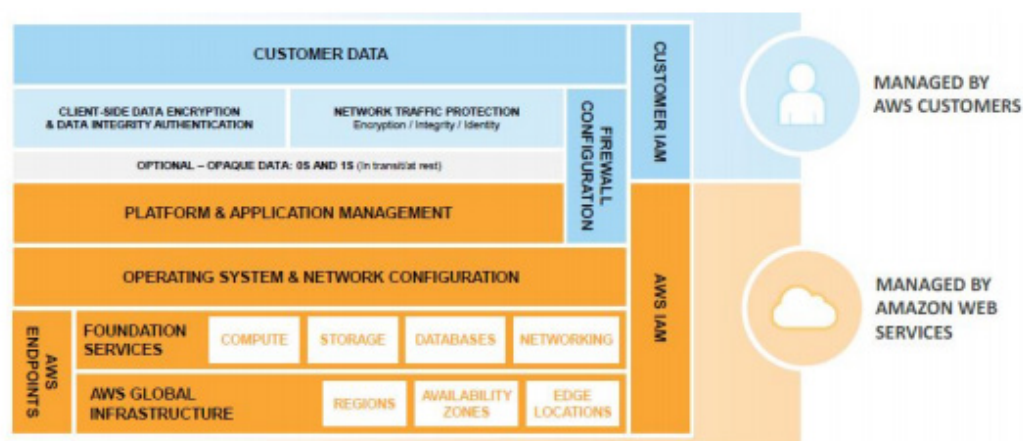


The Different Shared Responsibility Models

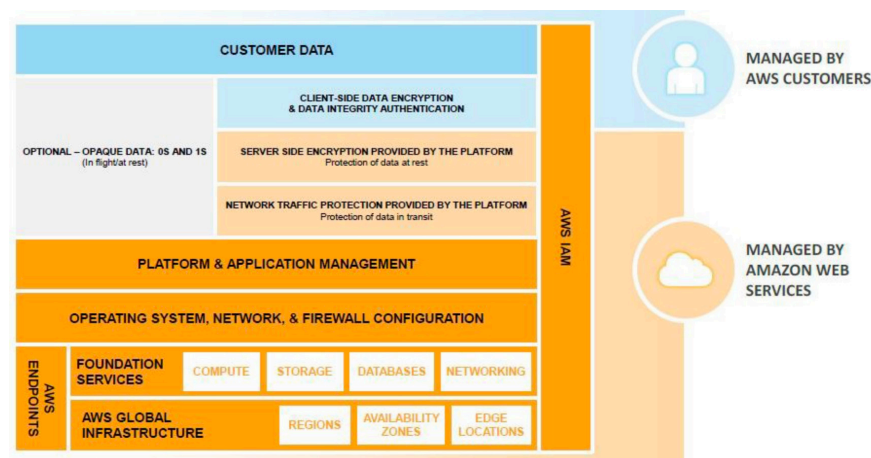
AWS has broken down the Shared Responsibility of their services into three models: infrastructure services, container services and abstract services. Azure and Google Cloud utilize similar models.



Shared Responsibility
Model for Infrastructure
Services.



Shared Responsibility
Model for Container
Services.



Shared Responsibility
Model for Abstract
Services.

Introducing Containers

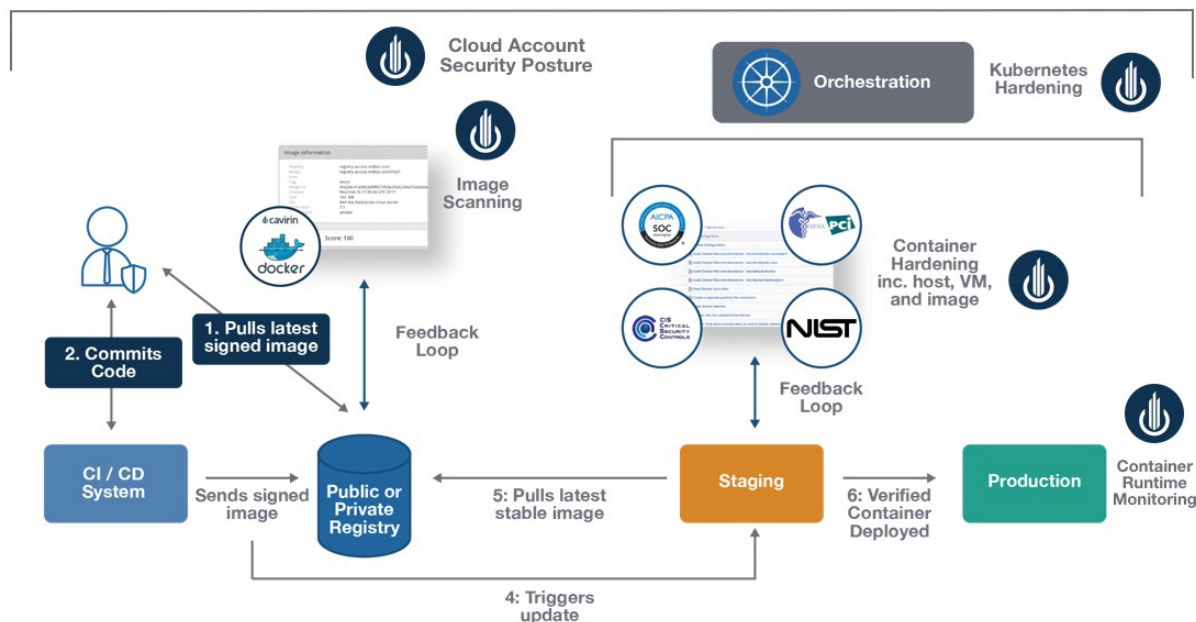
The Shared Responsibility also applies to container services. According to AWS, they are responsible for the platform (RDS), Guest OS, AWS infrastructure, as well as AWS foundation services. You are responsible for the data, the firewall rules and network access to the container service.

Containers invite the most concerning level of security from improper deployment and SQL injections. SQL injections are the insertion of unwanted/malicious code into poorly-designed applications and then passed to a backend database. It is the customers' responsibility to ensure that they are following best practices when introducing containers into their infrastructure.

**24 billions
containers
have been
downloaded &
there has been a
77,000% growth
in Docker job
listings.**

*DockerCon Europe
October, 2017*

Securing the container lifecycle



Cloud Security Posture Best Practices

Beyond protecting one's workloads, ensuring the proper security posture of the cloud account is critical. This includes not only locking down account access, but also monitoring any services consumed for unexpected events that could indicate an attack. Some best practices, focusing mainly on AWS but extensible to other providers, include:

- Comprehensive account level control: MFA, proper credential use, monitor and restrict services access, role-based access to applications
- Robust Identity and Access Management (IAM): timeouts, password policies, reduce groups in use, terminate inactive or unused groups, users, and roles
- Extensive security groups and network security: confirm proper configuration, lock down access to business requirements, network access control lists, restrict uncommon ports and unneeded common ports, cross-account access management
- Ensure Account 'Hardening: CIS AWS Foundations, Three-tier Web Architecture
- Continuous Monitoring: CloudWatch, CloudTrail, GuardDuty, active logging, validation, and access control, encrypt logs, audit, flow, and access logging
- Monitor the various AWS services utilized via CloudTrail, CloudWatch, Inspector, and GuardDuty.
- Utilize Trusted Advisor, particularly for AWS, to check the state of security groups, permissions, IAM use, MFA, as well as EBS and RDS public snapshots.



Beyond The Shared Responsibility Model(s)

The shared responsibility model is a great place to start, but it's just a starting point for building and securing hybrid workloads. Enterprises need to leverage the NIST Cybersecurity Framework (CSF). The NIST CSF provides a good framework as to how to ultimately reach better security, in this case within the Hybrid Cloud, but leaves it to the organization to decide upon what steps to take, and how. It also references a wealth of external guidelines and best practices but does not dictate which to use and to what extent. Finally, when trying to secure your hybrid cloud environment, it's important to adopt a defensive posture. Since data flows through the network as the lifeblood of your business, you now need to learn how to adopt an effective CyberPosture that defends you from today's security threats.

Just as it's important to understand and address the customers responsibilities in the shared responsibility models, it's just as critical to seek CyberPosture platforms and tools that verify public cloud security, protect private cloud assets and workloads, ensure your compliance audit preparedness and constantly deliver the status of your CyberPosture to your CISO in great detail using rapidly understood dashboards.

**Data security,
compliance/
governance,
and cloud pro-
vider lock-in
are the top
three cloud
migration
concerns**

*Bain and Morgan
Stanley, 2016*

About Cavin Systems

Cavin delivers cyberposture intelligence for the hybrid cloud by providing real-time risk & cybersecurity posture management, continuous compliance, and by integrating security into DevOps. The Cavin platform combines automated discovery, infrastructure risk scoring, predictive analytics, and intelligent remediation to help organizations of all sizes leverage the cost savings and agility of the cloud without increasing operational risk or reducing their security posture. For more information, visit www.cavin.com or follow us at www.twitter.com/cavin.



2114 Ringwood Ave, San Jose, CA
95131 USA
408-200-3544
www.cavin.com
info.cavin.com