SECURITY COMPASS WHITEPAPER

Why You Need a Security-First Approach to Cloud Strategy

Security Compass

Organizations of all sizes are moving their software infrastructure to the cloud, more with all the digital transformation taking place across industries.

Rather than investing internal resources to host and manage applications, organizations are embracing popular cloud storage services. As businesses adapt to the cloud environment, they are also recognizing the potential benefits of cloud computing in terms of cost savings, collaborations, and the ability to innovate faster

What is cloud computing?

Moving to “the cloud” means different things to different organizations.

For software companies, it can mean offering a hosted version of their applications. For others, it can mean running applications on platforms hosted by a third-party.

> Cloud computing is a set of computing services, including data storage, servers, applications, and networking, that can be shared by multiple users and offers the near-instant ability to scale up or down as required.

Cloud services are offered in a variety of ways to meet the needs of different users. In addition to the Software-as-a-Service (SaaS) offering, cloud providers also offer organizations the ability to run their internally developed or acquired applications in the cloud. Infrastructure-as-a-Service models allow organizations to run and deploy in-house and commercial applications on systems provided by the cloud provider, including hardware, storage, and networks.

Platform-as-a-Service model presents a different type of offering by providing development environments, services, and tools for users.

What about cloud computing security?

Although there are multiple benefits of cloud computing, some organizations have also shown concerns about the risks associated with cloud migration.

Moving to the cloud is not inherently less secure, or more secure than hosting applications in an owned data center. The biggest difference is that the Cloud Service Provider (CSP) is responsible for some aspects of security, and the cloud user or customer is responsible for others. Further, this responsibility changes depending on the deployment environment. Therefore, understanding which party is responsible for security for each portion of the deployment is critical.

Shared responsibility for cloud security

Cloud providers, like Amazon Web Services (AWS), Microsoft Azure, and others, work under a "shared responsibility" model for security.

They provide and manage the hosting facilities, physical hardware, and network infrastructure, thereby offering security, redundancy, and on-demand scalability for the customer's applications. This can include load balancing and fail over and network security infrastructure including intrusion detection/prevention and scalable VLAN.

Cloud customers, of course, are ultimately responsible for the security of their cloud-based applications. Therefore, understanding the shared responsibility model is critical. The model can be different for each application and cover the infrastructure, metastructure, infostructure, and applistructure layers of the environment. For example, in a SaaS service model, the cloud provider is responsible for securing the infrastructure and may provide Identity and Access Management (IAM) services. The customer, however, is responsible for securing the application and managing the IAM permissions.

As the service model used by a cloud customer moves from IaaS to PaaS to SaaS, the cloud provider takes on more of the responsibility for security.

When security fails

The shared responsibility model requires organizations to understand their responsibilities for each application and deployment and incorporate controls into the design, development, and testing of each application. This extends beyond the typical application security concerns of eliminating coding errors that can result in security vulnerabilities like SQL injection and cross-site scripting.

> "Through 2023, at least 99% of cloud security failures will be the customer's fault."
>
> **- Gartner Magic Quadrant for Cloud Access Security Brokers, October 2018**

Since cloud deployments leverage automation heavily and may involve more people in deployments than a traditional scenario, identity and access management, logging, and monitoring require more attention.

While the Center for Internet Security (CIS) publishes benchmarks and best practices for organizations deploying on each of the major cloud providers, these are not always followed. A recent study by RedLock found that on average organizations fail 30 percent of the CIS benchmarks and that 27 percent have experienced potential compromises.

The results of failing to configure cloud services correctly are easy to find:

- Hackers stole data on over 7 million users from an unprotected database of the National Payments Corporation of India.
- Records on over 540 million Facebook users was stolen from two unprotected Amazon S3 buckets managed by Cultura Colectiva.
- The US National Security Agency (NSA) left over 100 GB of data exposed on an Amazon s3 bucket configured to allow public access.
- An unprotected server allowed public access to information on over 93 million citizens of Mexico.

Security-first approach to cloud computing

Moving to the cloud requires organizations to rethink all aspects of application security. The Cloud Security Alliance (CSA) security guidance divides the secure development lifecycle into areas of responsibility with recommendations for each:

Secure Design and Development: Developers, security, and operations need to understand the shared responsibility model for each application, CSP, and deployment option and build this into requirements, designs, development, and testing.

Secure Deployment: Cloud deployments often use automation for testing applications in the deployment pipeline. In addition to testing for coding errors that can result in security vulnerabilities like SQL injection and cross-site scripting, tests should be added to account for API calls to the cloud service. In a containerized environment, vulnerability scans to ensure the security of the containers' base image should be added.

Secure Operations: Cloud environments are managed through APIs and a CSP-provided management interface. Security considerations include locking down the management plane for production environments and monitoring the environment for changes from approved baselines.

The CSA also provides a simple process model for managing security in cloud projects. As with any good security process, it starts with understanding security requirements, the architecture for an application, and the "shared responsibility" model used by the cloud provider and service offering.

- **Identify security and compliance requirements:** The first step in any security process is to understand the criticality of the application to an organization's business goals, the security policies for the application, and any applicable security or privacy regulatory requirements like GDPR, PCI-DSS, FEDRAMP, HIPAA, or PIPEDA. Many organizations will categorize or "risk rank" their applications, then apply specific security policies.

These, along with regulatory standards, will provide specific actions and controls that need to be addressed under the shared responsibility model. Teams should include CIS benchmarks as part of this exercise.

- **Select the provider, service, and deployment models:** Organizations need to understand their internal capabilities and those of the providers and select a provider and service model based on those capabilities. It is critical in this step to understand the shared responsibility model offered by the cloud provider in detail.

- **Define the application's architecture:** Since an application's architecture defines its attack surface, security must be part of any design review. Additionally, studies show that majority of the threats to an application can be derived from its development stack including programming languages and frameworks, deployment environment, along with applicable internal security policies or regulatory standards.

- **Assess the security controls, identify gaps and additional required controls:** With the requirements and threats defined, teams next map each risk or threat to a corresponding control. In a cloud deployment, and depending on the shared responsibility model, these controls may be an obligation of the cloud provider, development, security, or DevOps. It is therefore critical to also detail specific actions for validating each control.

- **Manage changes over time:** The adoption of rapid development methodologies like DevOps and CI/CD mean that applications are changing constantly – often several times each day. In this environment, security can be temporary. Security teams need to monitor the threat landscape over time, and operational teams need to be aware of changing configurations.

Go Fast. Stay Safe.

Cloud deployments are defined by speed and automation. By taking a “security-first” approach to cloud deployments, your teams can identify security requirements, threats, and controls before building software and thereby ensure that the shared responsibility model works well.

Secure software will continue to grow in importance through a combination of customer demand and regulatory pressure especially for cloud environments. The old choice between “fast and risky” or “slow and safe” for development is no longer adequate.

By adopting a balanced development approach, organizations can choose a “third way” — fast and safe. Our balanced development automation solution, SD Elements, identifies security weaknesses early in the development process and allows organizations to avoid common vulnerabilities. This means that security testing is primarily validating that prescribed controls were implemented correctly instead of acting as a primary vulnerability discovery activity.

The result is a balance between speed and safety. If you want to learn more about how you can secure your presence in the cloud, please get in touch with us.

SecurityCompass

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt balanced development automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on how organizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
1001 Bayhill Drive
2nd Floor
San Bruno, California
USA 94066

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001