Cloud Security –Foundations & Essentials

Today, digital is everywhere cloud, mobile, social and the Internet of Things are changing the way businesses operate. The rapid move to the cloud by organizations has passed a tipping point and the benefits are clear flexibility, agility, cost savings, future-proofing and more. Digital transformation is introducing and driving heterogeneous cloud adoption within enterprises, including private cloud, public and hybrid cloud, software-as-a-service applications etc.

This inescapable trend however raises many challenges for organizations as cloud applications lack consistent visibility, security, compliance, and control. Individually, some cloud providers have introduced limited controls that allow customers to define and enforce security within a specific cloud application. However, the approach to security from the cloud vendors in many cases is different from one another. In addition, all cloud provider security policy enforcement suffers from a major flaw it requires the enterprise to maintain policies and apply security controls separately across multiple different platforms with different interfaces and workflows, creating siloes of security, inconsistent cloud security enforcement, and costly administrative overhead. Addressing this requires a cross-cloud security approach that can mitigate risk of expanded attack surfaces across on-premises and multiple cloud environments.

BUSINESS CHALLENGES

Public cloud-based software as a service (SaaS) has become a common delivery model for business applications, including office applications and sales-and-marketing software etc. in use at enterprises. As a result, business groups and employees, external partners and customers require IT organizations to support a diverse set of cloud-based SaaS applications. Additionally, there is large scale use of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) solutions. Popularity of cloud-based applications, platform and infrastructure stem from the following business requirements:

- **Quick Adoption**: Business units looking for quick adoption of new applications as well as quickly change from one application provider to another.
- **Cost Benefit**: Short term cost-effective licensing
- **Effective Collaboration**: Business groups looking to collaborate with partners and customers, suppliers, subsidiaries and acquisitions

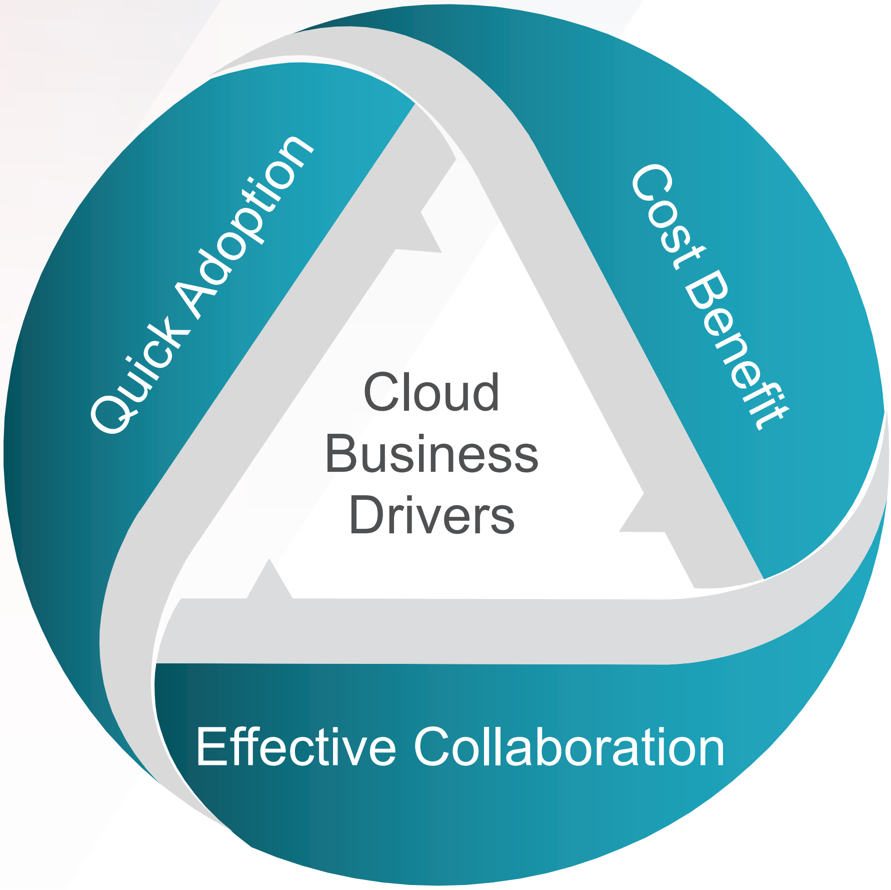

Figure 1. Follow the instructions in the figure above to insert SEO data.

KEY SECURITY AND PRIVACY ISSUES

Although emergence of public cloud computing is a relatively recent paradigm shift, insights into critical aspects of security can be learnt from experience of existing adopters, and from security researchers experimenting with available public cloud services and associated technologies. Some of the key security and privacy related issues are discussed below.

App & Data Security
Identity & Access
Gov. & Compliance

Figure 2: Key Security & Privacy Issues in the Cloud

Application and Data Security

While organizations adopt the cloud, one of the important concepts they need to understand is that security in the cloud is a shared responsibility, where the cloud service provider needs to ensure that the service is inherently configured and the organization – cloud consumer, needs to ensure that they also require application and data security. Application Security typically covers two areas:

- ***Configuration settings*** of each of the cloud services being adopted. This includes ensuring that the cloud service has both secure default settings and organization-specific settings for compliance.
- ***Cloud usage*** either
    - By a user or
    - As part of an integration with other cloud applications.

A data security risk is the exposure of data in the following two states.

- ***Data at Rest*** refers to data stored on an external cloud provider. Organizations need to ensure they understand the risk associated with relying on the cloud provider and need to verify that the provider acts as a true custodian of their data. As data owning organization, they need to proactively ensure data assurance by a cloud provider and put an appropriate security control that allows them to remain in charge of security of their own data.

- ***Data in Motion*** refers to data as it is moved from a stored state to a different location. Any time data is uploaded to be stored in the cloud or downloaded by user to his/her computer or mobile device, it is considered to be *data in transit*. Encryption is a form of protection for *data in motion.*

Identity and Access Management

Understanding and defining user authentication and authorization among cloud actors is a key aspect of cloud security. Without knowing who is logging in to the cloud-based information system, and who is accessing what data a cloud eco-system cannot be protected.

- ***User Authentication*** is the process of establishing confidence in the identity of a user, typically by entry of a valid user name and a valid token (password, key, biometric info) for the purpose of granting access to information system or resources. Authentication assurance levels should be appropriate for the sensitivity of the application and information assets accessed and the risk involved.

- ***Authorization or Access Control*** is the process of enforcing policies such as determining what resources or services a user is permitted to access. Typically, authorization occurs within the context of authentication. Enforcing authorization policies is critical in a cloud eco-system.

- ***Identity Federation*** allows organization and cloud provider to trust and share digital identities across both domains and provides a means for single sign-on across cloud services. Clear separation of cloud consumer from those of the cloud provider must be ensured to protect consumer's resources from cloud-provider authenticated entities.

Compliance, Governance and Trust

Compliance refers to responsibility of an organization to operate in agreement with established laws, regulations, standards and specifications, and a business must abide to these. The requirements can be external or internal, and are driven by business objectives, customer contracts, laws and industry regulations, internal corporate policies and other factors

MAKE A SECURE TRANSITION TO PUBLIC CLOUD

Oracle recognizes the growing demand and business adoption of cloud services. The following multi step approach and characterization is derived and adapted from work by NIST and International Organization for Standards (ISO), and can be used for addressing cloud security challenges within your organization.

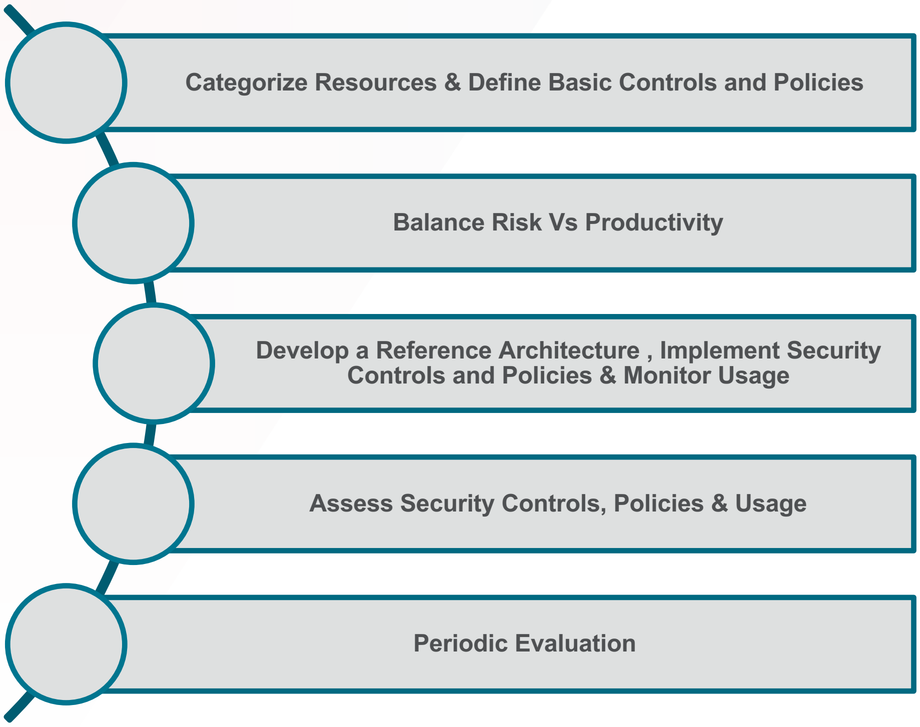
Categorize Resources & Define Basic Controls and Policies
Balance Risk Vs Productivity
Develop a Reference Architecture , Implement Security Controls and Policies & Monitor Usage
Assess Security Controls, Policies & Usage
Periodic Evaluation

Figure 3. Steps involved in making a secure transition to the cloud

Categorize Resources & Define Basic Security Controls & Policies

The goal of the step is to establish criticality and sensitivity of cloud resources and associate risk levels with them. Risk levels may be computed based on the kind of access, data and users accessing the application. Additionally, application risk scores can also be computed based on external factors such as the reputation of the cloud application.

SELECT SECURITY CONTROLS: Security controls are countermeasures or safeguards to prevent, counteract or otherwise respond to security risks. These are settings per cloud service that ensure that a minimum desired security is in place. Security controls should be selected to map to risk levels associated, based on categorization of the respective cloud resources. These controls secure the state of the cloud service at any given point in time. For example, security controls for an AWS instance needs to ensure that all S3 buckets are encrypted. If encryption is turned off, it inherently reduces the security of the organization.

APPLICATION AND DATA SECURITY CONTROLS

Application level security controls are essential to ensure that each application matches the organization’s security needs and mandates. For example, if the organization has adopted Office 365 for collaboration, Amazon Web Services (AWS) and Oracle Cloud Infrastructure (OCI) for IaaS and Oracle HCM Cloud for HR Management, each of these applications need to be configured appropriately. Each of them provides multiple services, for example, IaaS have compute, network, storage and security services, Office 365 has Exchange, OneDrive etc. Getting subject matter experts in each area to ensure that the right configuration is in place is a challenging task. Moreover, all these being cloud application, there is inherent advantage to leveraging network effects, that is, learning from best practice deployments of other organizations.

In cloud, encryption is a primary means to protect data at rest and between storage and processing phases. An organization needs to ensure that keys used in encryption are stored securely and managed appropriately.

IDENTITY AND ACCESS MANAGEMENT (IAM) CONTROLS

Identity and Access Management is a key element in the security of an operating cloud and is usually the first level of control in a defense-in-depth strategy of an organization. Controls must protect confidentiality, integrity and availability of identity information and will support needs for authenticating cloud personnel. An identity management system should allow for identity portability for the users and presents a single Mechanism for internal access as well as tenant and user access. The federated identity management system should allow for interoperability with customer and third-party identity providers as possible.

Specific controls for IAM need to be put in place. Some of the basic controls such as password policies, the need to strong Multi-factor Authentication (MFA) to sensitive data access and for highly privileged operations, calculating the risk of the user, application and the data in use, are necessary.

Authorization mechanisms for cloud management should be constrained and not allow cloud-wide access. Such authorization mechanisms typically extend to activities that user may perform on the cloud application and are controlled by policies.

Any solution that helps you leverage such best practices, provides as many controls per cloud service out of the box and provides visibility into any changes that may happen will enable an organization to achieve a secure cloud posture quickly.

Balance Risk Vs Productivity

The key for organizations is to have a comprehensive cloud security strategy. The ROI for security measures should be as easy to explain, as the value of a new cloud service that a business unit is trying to adopt.

Determine whether controls are sufficient and appropriate and if they provide adequate protection against anticipated threats along with a plan for risk mitigation. A focus on making security measures easy to use, implement and maintain can balance security and productivity. A goal should be to empower users to be productive and yet have an understanding of risks. Strive for simplicity and burden of security will lessen, allowing users to be more productive.

Risk scenarios should be developed as joint effort between subject-matter experts and information security specialists. Security controls shouldn’t be viewed just as a static configuration, but rather with a scalable design – one where any instance of the service that is invoked provides the same risk posture and such that when a vulnerability is discovered, appropriate action can be taken to fix the design.

Develop a Reference Architecture, Implement Security Controls & Policies and Monitor Usage

This stage typically requires the involvement of broader application and security teams to ensure that the right applications and interfaces are being used. They also ensure that the services are configured based on the security controls that have been defined in the previous step. Additional policies may also be implemented to suit the organization's needs.

Another important step in this stage is to ensure that usage of these cloud services is in line with the policies and security needs. This is typically provided in two phases:

- **User Behavior Analytics** – Leveraging Machine Learning (ML) techniques, it is possible to determine the risk of a user. This takes into account multiple factors that are generic – such as the device that the user is using, the location of the user etc. and cloud service-specific – such as the number of instances of an IaaS service that the user consumes on a regular basis.
- **Suspicious Behavior** – This is typically based on usage patterns of the user. For example, we may determine that there are too many failed login attempts or that the distance between two consecutive logins for a user are suspicious.

As is obvious, this stage should be used to ensure that the right risk events are flagged per application and that there is a mitigation path.

Assess Security Controls, Policies & Usage

This step is used to determine the effectiveness of implemented controls and involves verifying that the controls are implemented and operating as intended. Typically, all the controls and policies result in risk events. These risk events need to be monitored to ensure that they are appropriate, informative and actionable. In many instances, the initial phase of implementation may result in noisy risk events. The cloud security solutions in use must now be tuned to ensure that the resultant risk events are appropriate. Most organizations integrate with an incident management solution to ensure there is a workflow to remediate risk events.

Periodic Evaluation

Technology is moving fast in the cloud world, and your business is probably too. Your cloud security needs to evolve at the same pace. With an ever-changing and evolving cloud ecosystem, security measures must be reviewed on a periodic basis and updated. Cloud service providers introduce multiple new services and fine tune the settings of existing ones. An organization needs to ensure that it is nimble enough to adapt to these changing circumstances and that the security controls, policies and configurations they maintain do not compromise their cloud security posture.

CONCLUSION

Oracle CASB Cloud Service provides all the elements to help you make a secure transition to the cloud. It acts a first line of defense and provides security controls and policies to ensure that any cloud service being has the appropriate configuration and control. It leverages the industry's best user and entity behavior analytics (UEBA) capabilities to deliver insights into cloud usage and take appropriate mitigating action.

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

Oracle is committed to developing practices and products that help protect the environment