



Predict | Protect | Prevent

The background of the slide is a dark red and black abstract graphic. It features a faint world map, binary code (0s and 1s) arranged in circular patterns, and a large, glowing white padlock icon in the center. The padlock is surrounded by a circular border of binary code. The overall theme is cybersecurity and cloud governance.

# ARCON | Cloud Governance

# Overview

Every industry in the post-pandemic era is undergoing unprecedented innovation, relying heavily on cloud platforms and software-as-a-service (SaaS) apps. But why this sudden demand for transition?

- Anywhere accessibility; any device accessibility
- Centralized security features/ practices
- Higher qualitative and quantitative performance
- Get rid of On-Prem software and hardware maintenance.
- Quick deployment of applications
- Better Business continuity and effectiveness
- Faster IT operations and business processes
- Value for money

Dynamically, all the benefits (even more than the above) of CIEM (Cloud Infrastructure and Entitlement Management) architecture are luring organizations for a paradigm shift from on-prem IT infrastructure to multi-cloud or hybrid cloud environments. The rapid adoption of multi-cloud platforms by global enterprises is completely changing the Identity and Access Management (IAM/ IDAM) fabric including the identity governance and entitlement policies.

It is observed that almost three out of four business enterprises adopt cloud or multi-cloud platforms. It helps them to meet the requirements arising from increasing daily IT computational, operational and infrastructure use cases through various cloud platforms such as AWS (Amazon Web Services), Azure and Google Cloud. Moreover, there is significant growth of cloud access vulnerabilities such as insider and third-party threats as it provides unified access control mechanisms for the cloud users along with rule and role-based policy enforcement.

The question here is how to ensure security and governance of the identities and access control mechanisms across these multi-cloud environments. Because transition from on-prem to cloud environment could create new vulnerabilities that could be the secret door for cloud infrastructure misuse.

With hundreds or thousands of human and non-human (digital) identities accessing cloud resources, consoles, and workloads for day-to-day use cases, the emerging IT security challenges have left enterprises open to data breach risks. It is not just human identities that need to be protected, but machine identities/non-human identities (devices and cloud workloads such as scripts, containers, VMs, CI/CD tools, RPA tools) must be controlled and governed.

Furthermore, the global regulatory compliance standards such as FedRAMP, NIST, GDPR, and SOC2 explicitly demand provisioning and deprovisioning of users while following the least privilege principle along with many other access control mandates.

# About ARCON | Cloud Governance solution

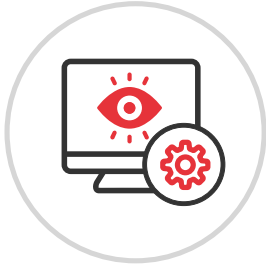
ARCON | Cloud Governance is a centralized solution model that helps in visualization, manages, monitors, and controls identities and resources across multiple platforms in cloud environments. It provides the necessary IT oversight for users and non-human identities in a cloud environment. It can discover and track the identities and entitlements in the cloud environment and control them in line with the enterprise security policies.

With the help of its native AI/ML-based algorithms, ARCON | Cloud Governance solution helps to assess policy updates to remove excess or unused entitlements and help in provisioning/deprovisioning them to users, groups, non-human entities. The platform assesses unwanted or underused access across all IaaS platforms. This solution also offers a dynamic access control policy where privileged rights can be revoked automatically or on-demand, after the completion of specific tasks. This helps cloud security administrators to restrict any-time access of specific users (e.g. developers) who are using CI/CD workflows and other services in-cloud.

## ARCON | Cloud Governance

# Key Features

ARCON | Cloud Governance solution offers complete control over the IT workloads in cloud infrastructure by enforcing robust access control policies across the cloud infrastructure. Here are the feature details.



### Granular Visibility

Security administrators can have comprehensive visibility over cloud entitlements with this feature. It offers a graph view of all end users' access that denotes the relationship between identities and their corresponding entitlements. Thus, administrators can weigh permissions, helping them to make well-informed decisions for high-risk identities and entitlements.

### Centralized Dashboard

Provides administrators with a 360-degree view of all the cloud resources with a single pane of glass. Offers interactive dashboard for comprehensive overview of various entitlements available across the multiple cloud platforms which includes an ability to govern the cloud entities, enabling administrators to easily identify and manage risky entities.



### Entitlements Management

It strengthens the security fabric on cloud as administrators can define the policies and permissions for distinct entities wanting to access platforms with JIT entitlements/roles /privileges.

### Risk Control

It offers holistic risk management. The built-in AI and ML capabilities enable administrators to analyze and categorize permission usage, detect shadow administrative rights and overprivileged permissions, and generate risk scores for further action.



### Governance of SaaS platforms (Provisioning/ Deprovisioning)

Cloud Governance offers robust governance engine for identity lifecycle management, ensuring review provisioning and deprovisioning of privileges. Identity governance enforces strong accountability so that privileges do not spiral out. In addition, comes with pre-built integrations with an array of SaaS platforms such as GitLab, Okta, Salesforce, Atlassian, Office 365, Dropbox, and many others to accelerate cloud adoption.

## Compliance with IT standards

Meets with global regulations and IT standards that demand stringent compliance as to data protection, data integrity, data security. For example, SWIFT, PCI-DSS, NIST, HIPAA, GDPR, American Institute for of Certified Public Accountants SOC for cybersecurity.

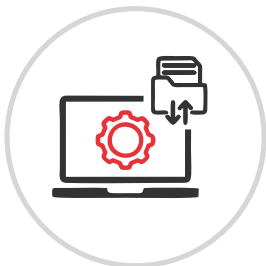


## Dynamic Access Control Policy

This solution offers a dynamic access control policy where privileged rights can be revoked automatically or on-demand after the completion of tasks.

## Control of Over-Entitlements

Over-entitlements in a multi-cloud environment could be highly catastrophic as they increase the chances of unauthorized access and anomalous activities. Misuse of over-privileged rights in the cloud environment could invite unprecedented IT threats. Cloud Governance solution controls over-entitlements (Provision/Deprovision policies, groups) by following the 'Least Privilege' principle.



## Data Access Governance (DAG)

ARCON Cloud Governance once integrated with ARCON My Vault, offers robust Data Access Governance (DAG) module that builds data visibility across multiple shared folders and ensures data integrity and desired data confidentiality. It provides end-to-end data encryption and meets compliance requirements with the global and regional IT standards.

ARCON | Cloud Governance

# Benefits at a glance

Provision/ Deprovision of excessive entitlements/ standing privileges/groups in the cloud environments.

Generates Risk Score & Granular level AI/ML-based recommendations to remediate risks emanating from cloud entities (IAM users, groups, service principals, roles, service accounts etc.)

Offers comprehensive visibility over multi-cloud platforms in a single dashboard

Ensures instant policy enforcement and remediations to detect IT threats

Mitigates insider and third-party threats seamlessly

Builds weightage of permissions with interactive graphs for each entity

Strengthens regulatory compliance framework



# About ARCON



**ARCON** is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

All rights reserved by ARCON

This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner's exclusive rights will be considered unlawful and might be subject to penalties.