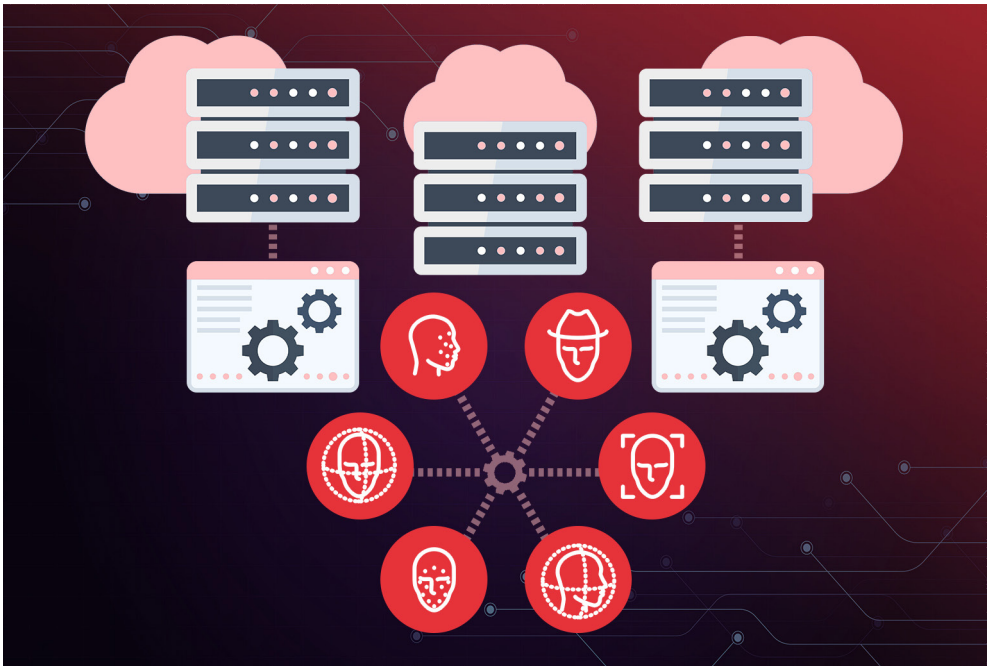
The Role of Identity Governance in ever-expanding IT Environments



In the vast and distributed IT environment along with ever-increasing number of IT users, organizations are repeatedly challenged by the identity abuse threats. A robust identity governance ensures the right end-users access the right resources at the right time for the right purpose, protecting IT assets from breaches and unauthorized access.

Table of content

An Overview

Protecting identity in increasingly complex IT environments is challenging. The challenge arises from the fact that today's organizations have a widely distributed IT environment. Users, endpoints and applications have not just exploded in numbers but those IT components are widely distributed in multiple cloud platforms, distributed across datacentres and managed service environments.

Therefore, identity governance is becoming increasingly important to organizations. Identity governance ensures that all identities are being discovered, mapped, allocated (based on users' responsibilities), controlled and monitored. A robust identity governance framework ensures seamless lifecycle of identities, reduces chances of breaches and identity abuse along with providing a strong foundation for Identity and Access Management.

In this whitepaper, we have discussed various use case scenarios where identity governance becomes a critical component to ensure overall robust Information Security posture.

Identity Governance in Multi Cloud Platforms

More and more organizations find merit in managing, computing and s toring resources on-cloud as it optimizes the productivity thanks to scalability, operational efficiency and financial benefits offered by this model. However, from an identity security perspective, migrating data to on-cloud environments comes with its own set of risks and compliance issues.

Although major cloud platforms do offer a set of pre-defined access control policies, those policies are not adequate to address security challenges. Moreover, many of those policies are complicated, literally making cloud console admins tasks difficult to handle a large number of access control requests in a fine-grained manner. In addition to cloud managers who have access to everything, organizations have a responsibility to manage and control access of their own cloud console admins, developers who are using DevOps and other services on-cloud along with a wide range of business and IT functional users, who could be a third-party.

Another access control challenge that often faced is the sudden increase in the number of overprivileged users as organizations adopt multi cloud platforms. By default, admins with administrative console rights literally become the super users with complete authority over cloud resources.

These overprivileged users with excessive entitlements have complete control over creating, deleting or changing storage and network configuration. If those over entitlements are not revoked on time, there is a strong change of breaches and other malicious activities.

Identity Governance in Distributed Data Centre Environments

Large banking and financial institutions often have workloads and data spread across multiple data centres. Identity governance can become a major challenge if organizations lack a centralized governance structure to manage a large number of identities in distributed environments. When there is an absence of unified governance, invariably the IT infrastructure becomes fragmented and starts operating in silos. The proper controls around each identity through a fine-grained access approach and risk analytics become an uphill task in a non-centralized IT environment, as there tends to be ambiguity around people's roles and access control policy. A centralized administration of users along with provisioning of users is critical to prevent misuse of identities, credentials and possible breaches.

Identity Governance in ever-expanding hybrid environments

The impact of pandemic along with increased pace of digitalization has necessitated the importance of robust identity governance in hybrid environments. A typical IT setup of modern-day enterprises include a wide range of use-cases that requires security and risk management teams to continuously establish an identity trust: Some of the examples include:

1. Developers' requirements to access APIs, microservices, DevOps environments
2. Business managers, Sales teams and Account Management teams requiring access to marketing automation and CRM tools
3. Network admins requiring access to change network devices' configuration
4. Privileged users like database administrators requiring access to the critical infrastructure that includes a host of applications and database
5. Systems administrators requiring to change, alter, or delete configurations or install software and conduct other administrative tasks

6. Social media administrators requiring access to corporate social media accounts
7. Third-party consultants responsible for day-to-day IT operations and functional tasks

Monitoring hundreds of identities operating both remotely and on-prem, including permitting and restricting (access) for a wide range of identities in hybrid environments is possible only through a well-defined identity governance policy. With the help of identity governance, the IT security team can evaluate employees' entitlements to access IT resources and revoke rights of suspicious ones from the list. Identity governance and management eases IT administrative burden as role and rule-based access policies establishes the access control framework and accelerates technology adoption.

Identity Governance in Managed Service Provider (MSP) Environments

Ensuring the security of digital identities is a major challenge in the MSP environments. MSPs typically host hundreds or thousands of clients' data in multi-tenant cloud and on-prem data centres, which means there are inherent risks. Entitlements can be misused or abused if there are no proper safeguards to ensure identity governance. Moreover, many clients also opt to run IT services that demand privileged access to critical applications, codes and databases. Robust identity governance, in the case of MSPs, constructs the accountability framework that offers a mechanism to manage and control the user entitlements;, that is roles and responsibilities in a fine-grained manner along with session monitoring and reporting of all access to resources.

Reinforcing Identity Governance with ARCON

ARCON offers best-in-class solutions that enable IT security professionals to build a robust Identity Governance framework around datacenters whilst enabling them to develop a comprehensive IT compliance framework. Our mission is to provide global organizations with a secure centralized platform for managing, monitoring and controlling the increasing number of digital identities. Therefore, ARCON strives to innovate and build highly scalable solutions to support enterprise access control use-cases- whether on-premises, on-cloud or in hybrid infrastructures.

Our robust stack of solutions ensures Authorization and Administration of each and every identity through an intuitive Workflow Matrix. Security features such as Multi-factor Authentication (MFA), Just-in-Time Access to IT resources, Granular Controls, Single sign-on (SSO), Session Monitoring and Management, User discovery, User mapping (for entitlements), Audit trails and reporting, Risk-based analytics including behavioral analytics on anomalous profiles simultaneously helps to reinforce the IT security posture, which builds the foundation for a strong Identity and Access Management framework.

Conclusion

A modern-day enterprise's IT environment is very complex from access control perspective. Amid increasing digitalization, the number of digital identities, end-users and devices are growing at a rapid pace. Against this backdrop, it becomes a challenge to monitor and control the end-users. Who accesses the systems? Why was it accessed? When was it accessed? Is the end-user authorized to access the systems? If these critical questions remain unanswered in the absence of adequate access control mechanisms in place, organizations risk data breach and credentials abuse from insiders and third-party consultants. To overcome these humungous challenges, ARCON provides Unified Access Governance Platforms that enables Information Security leaders to manage the complete lifecycle of digital identities.

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.

PAM: ARCON | Privileged Access Management (PAM) is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

UBA: ARCON | User Behaviour Analytics (UBA) is a highly effective risk predictive & analytics tool built for daily enterprise use cases. It breaks the traditional approach of 'restrictive' access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time.

SCM: ARCON | Security Compliance Management (SCM) allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

Connect with us