arcon

Predict | Protect | Prevent

Identity and Access Management

Introduction

Identity and Access Management (IDAM) is a critical IT security component that strengthens the overall IT risk management and compliance framework.

Against the backdrop of a large number of dispersed identities in a typical mid-size to large organization that require day-to-day access to systems, ARCON | IDAM enforces controlled IT environment where each identity is administered and governed.

Through ARCON | IDAM, the IT risk management and compliance team can ensure that end-users' runtime access to systems is managed through a unified engine and documented. The solution offers a strong security layer in front of IT security components such as web applications and APIs by enforcing authorization and authentication of identities.

ARCON | IDAM solution enables enterprise IT security teams to address a large number of daily use-cases

IT administrators find it more and more difficult to administer and govern identities when the number of end-users in an IT environment increases gradually. Managing end-user access to different applications becomes a challenging task in the absence of adequate access control capabilities. It not only impacts the IT administrative experience but also increases the risk of identity abuse/misuse.

ARCON | IDAM provides a robust solution to the problem statement by automating the end-users' identity management. The solution ensures Identity Lifecycle Management through provisioning, de-provisioning, workflow matrix, role and rule-based access among other access control capabilities.

The solution enables to address the following enterprise use-cases

- Management of machine identities
- Role-based access to business assets and infrastructure assets
- Access to multiple systems and infrastructures through federated identity management
- Secure and authorized access to legacy applications

ARCON | IDAM

Offers the following features

Access Control

The solution offers robust granular access controls that enables the IT risk management and compliance team to secure IT infrastructure. It is also to comply with several IT standards and regulatory mandates. ARCON | IDAM ensures fine-grained access control to business applications, network devices, infrastructure devices, thick clients, databases and Web applications through group-based and device-based access control, permanent access, one-time access, time-based access and blacklisting of end-users' access. The solution also supports just-in-time access to target systems.

Lifecycle Management

ARCON | IDAM solution provides end-to-end lifecycle management for each function i.e., Provisioning of a user on the application, updating the rights and accesses in case an employee is getting transferred to another department or his/her role is being altered. ARCON | IDAM can also deprovision a user from the end application if he/ she leaves the organization or no longer needs access to that particular application.

Identity Governance and Administration

Identity governance and administration is a proactive approach that safely controls the information of the employees, partners, clients, and provides authentication and authorization to the system - approved user identities. ARCON | IDAM will close all the security gaps and ensure rigorous guarding of the sensitive data in an impeccable manner for all the registered accounts in the organization. ARCON | IDAM streamlines automated provisioning and de-provisioning of the identities, along with faster auditing and reporting for all your users.

Single Sign-On

ARCON supports industry standards OpenID Connect and SAML and OAuth 2.0 for Identity Access Management, encryption and identity management, and authorization of resources. ARCON | SSO has a wide range of already developed connectors for web apps ranging from business applications to collaboration tools and so on. ARCON | SSO also offers a reliable integration for SSO to all your mobile applications and web applications, optimized for mobile platforms, with industry-standard SAML authentication and other modern protocols.

Auto-Onboarding Solution

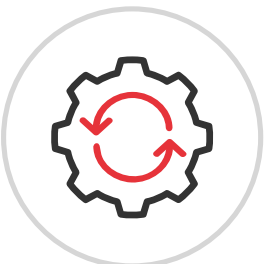
Auto-onboarding allows administrators to seamlessly and automatically add new server groups, and user accounts with associated privileges to map new users onboarded on ARCON | IDAM. It also helps administrators to auto-provision and de-provision users by interacting with the active directory. With auto onboarding, organizations can ensure that all information collected during the onboarding process remains confidential and far from any unauthorized access.

Authentication Federation

ARCON | IDAM can seamlessly integrate with various authentication repositories like Microsoft Active Directory, Azure AD, LDAP, and Source of Truth for user provisioning and management and share user credentials with other integrated cloud and on-premises applications. It also offers a local authentication repository wherein login credentials can be created for users.

Multi-factor Authentication

ARCON| IDAM supports third-party authentication tools to ensure additional security layers for systems. The solution integrates with authentication tools such as PRECISION, VOICETRUST, SAFARAN, GEMALTO, VASCO, 3M, RSA among many others.



Multi Conditional Workflow

No more tedious and long approval process. The Workflow matrix makes administrators' lives easy. It enables to configure the approval process for privileged users, user groups, and service groups. Service and password request workflow mechanism speed up the process of assigning target servers to privileged users.

Password Management

The end-user can easily manage the password of different applications. While configuring the service of an application, the user can set a complex password. This password can be updated manually by the end-user as well as can be rotated as per the defined policy. This also ensures proper synchronization across the network to prevent service disruptions. ARCON | IDAM users can customize and automate steps for any SSO activity with the use of RPA Bot (Robotic Process Automation Bot). It could be image-based control recognition, Shortcut keys, Control ID, etc. .

Reporting

The regulatory standards mandate the IT risk management team to provide detailed information about access control policies needed for safeguarding critical information. Moreover, regulators demand comprehensive audit reports about every privileged user's activity on critical systems. To meet this regulatory requirement, enterprises need to generate and maintain comprehensive audit trails of every privileged session. ARCON's robust reporting engine makes your security team audit-ready by providing customized and detailed analytics of every privileged access to target systems.

Session Monitoring

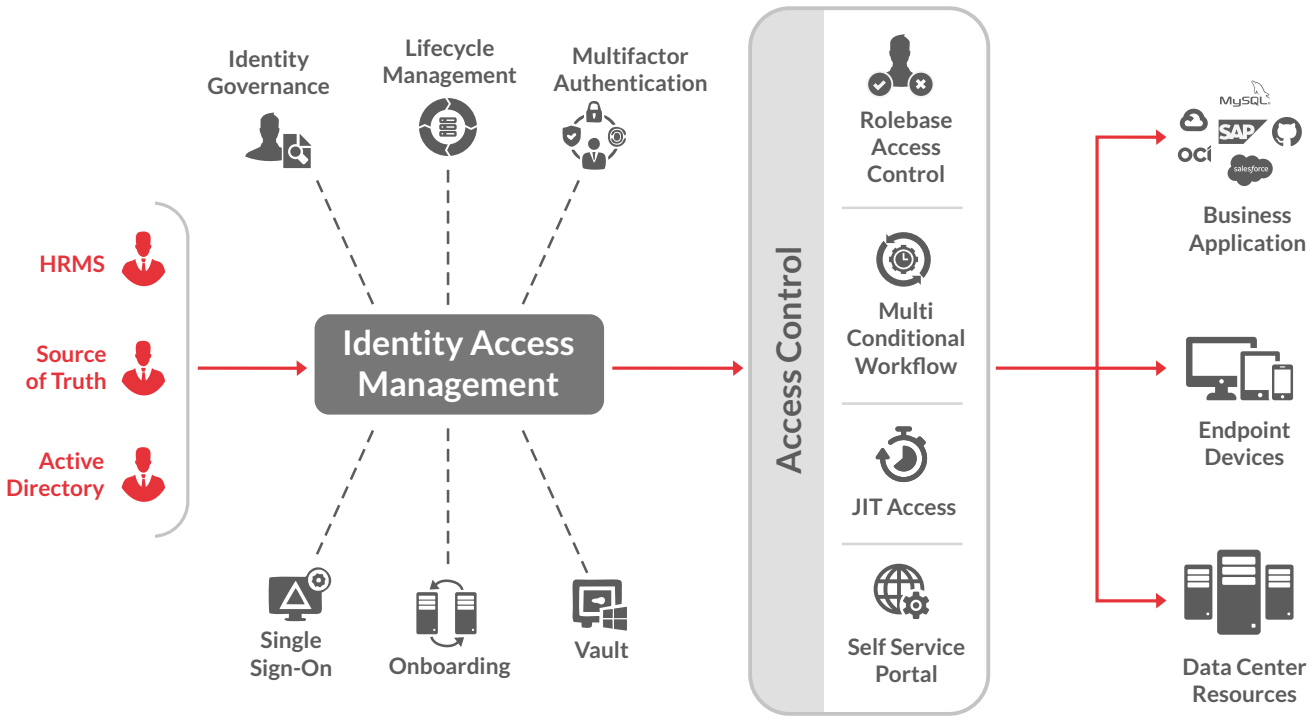
Session monitoring provides auditing and monitoring of privileged activities around the enterprise IT network. This feature enables the IT security team to spot any suspicious activity around privileged accounts. A live Dashboard ensures that all critical activities performed by administrators across the IT infrastructure are viewed in real-time.

ARCON | IDAM

Benefits at a glance

- Enhances enterprise digital experience by securely managing digitalidentities and entitlements of end-users and services
- A unified engine that provides complete view of all the access rights of all employees on all the platforms for better IT oversight
- Provides intuitive workflow matrix for IT administrative ease
- Offers complete life-cycle management of digital identities
- Seamlessly integrates with various authentication repositories like Microsoft Active Directory, Azure AD, LDAP, and Source of Truth for user provisioning and management
- No requirement for separate deployments of PAM, SSO and IDAM - a single one-time installation with all integrated features helps to avoid longer deployment worries

Architecture Overview



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.