arcon

Predict | Protect | Prevent

Privileged Access Management

Introduction

Privileged access management is at the core of cybersecurity requirements. Privileged access, as the term suggests, is administered by privileged users—administrators and users with elevated permissions—to access infrastructure and critical business assets. Therefore, any sort of privileged credential compromise or misuse resulting in unauthorized access to systems might cause a catastrophic IT incident.

As a result, privileged access management requires the utmost security. ARCON | Privileged Access Management (PAM) provides IT security and risk management staff with adequate security capabilities needed to manage, monitor, and control privileged users. The solution provides best-in-class security features and functionalities such as fine-grained controls, rule and role-based access, just-in-time privileges, multifactor authentication, password vaulting, session monitoring, customized reporting, and many other classic PAM capabilities to address some of the most complex use-case challenges found in privileged access management environments (hybrid datacenters, distributed datacenters, multi-cloud, and DevOps environments).

The solution enables IT security teams to comply with a host of IT standards such as PCI-DSS, HIPAA, SOX, and regulatory mandates such as the GDPR, as well as several regional and local mandates as prescribed by central banks and cybersecurity governing authorities with respect to data security, data protection, and data integrity.

Trusted by more than 1200 global organizations, ARCON | PAM is known worldwide for its product capabilities, swift integrations, lower total cost of ownership, and world-class IT support, consulting, and services. ARCON has been consistently named as a leading brand in the PAM space. Global analyst communities such as Gartner and KuppingerCole have consistently recognized ARCON as a leader in Privileged Access Management.

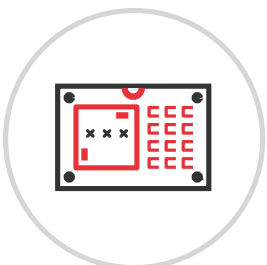
Features for

Security, Monitoring & Governance

Fine-Grained Access Control

Fine-grained access control in ARCON PAM refers to the capability of providing granular access control to privileged accounts based on specific roles, responsibilities, and tasks. It enables organizations to define and enforce precise access policies for privileged users, reducing the risk of unauthorized access and misuse of sensitive systems and data. With fine-grained access control, organizations can limit privileged users' access to only those systems, applications, and data that they need to perform their jobs. It also allows for the creation of policies that restrict the type of activities that privileged users can perform on a specific system or application. This way, organizations can maintain control over privileged access and ensure that access is granted on a “need to know” and “need-to-do" basis. Fine-grained access control is an essential feature of ARCON PAM, as it enables organizations to manage privileged access more effectively and reduce the risk of insider threats and cyberattacks.

Password Vaulting



ARCON PAM's password vaulting feature ensures that privileged account passwords are stored and managed in a highly secure environment by providing a secure and single point of control. ARCON Password Vault employs strong encryption algorithms, including FIPS-approved Advanced Encryption Standard (AES) 256-bit encryption. This protects the credentials stored in the vault from unauthorized access and ensures compliance with FIPS guidelines. Access to the vault is strictly controlled using strong access controls.

The credentials vaulting feature enables organizations to generate complex, randomized passwords for privileged accounts that cannot be easily guessed or cracked. It also allows organizations to enforce password policies such as password expiration and extent of complexity and rules to ensure that passwords are updated regularly and meet the organization's security standards. ARCON PAM's credentials vaulting eliminates the need for privileged users to remember and share passwords, thus lowering the risk of password theft and misuse. It also provides an audit trail of all privileged account password access, including who accessed the password, when, and for what purpose, thereby improving the overall security posture of the organization.

Session Monitoring

Session Monitoring is a feature of ARCON Privileged Access Management (PAM) that provides real-time monitoring and recording of privileged sessions. Organizations can use Session Monitoring to monitor privileged user activity in real time, allowing them to detect and respond to security threats quickly and effectively.

Session Monitoring records a detailed audit trail of all privileged user activity, including all commands fired and actions. This audit trail is securely stored and can be searched and analyzed at any time for forensic analysis and compliance reporting purposes.

ARCON PAM also includes real-time alerts for suspicious activity, enabling security teams to respond to potential threats quickly by freezing or terminating the session. This feature adds an extra layer of security to privileged accounts and helps to protect sensitive data.

Session Monitoring feature allows real-time monitoring of privileged sessions by capturing keystrokes, mouse clicks, metadata, processes, and other privileged user activities which allows security teams to monitor, record, and audit privileged access activities.

arcon

Multi-factor Authentication

ARCON PAM supports several MFA options, including ARCON Authenticator App, Email OTP, SMS OTP, hardware tokens, TOTPs like Google and Microsoft Authenticator, biometric authentication, Facial Recognition, and many more. Organizations can select the MFA solution that best meets their security needs while also seamlessly integrating with their existing IT infrastructure. ARCON PAM can also integrate with third-party multi-factor applications such as Cisco Duo, etc.

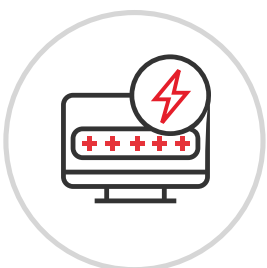
ARCON PAM's MFA (Multi-Factor Authentication) feature is designed to meet the requirements of the Payment Card Industry Data Security Standard (PCI-DSS). PCI-DSS is a set of security standards designed to assist organizations that process, store, or transmit credit card data in maintaining a secure environment. ARCON PAM's MFA solution can assist organizations in meeting this requirement, which is a key component of the PCI-DSS standard.

SSH Keys Management

SSH key management is an ARCON PAM feature that allows for the secure management of SSH (Secure Shell) keys, which are used for remote authentication and access to servers and other devices. It aids organizations in maintaining control over SSH keys by serving as a centralized repository for key storage, management, and distribution.

ARCON PAM's SSH key management feature automates the process of generating time-based keys and rotating SSH keys, allowing organizations to manage access to sensitive systems and applications in a secure manner. It also provides detailed reports on key usage, allowing administrators to monitor and audit key resource access. This aids in the prevention of unauthorized access and the defense against cyber threats such as SSH-based attacks.

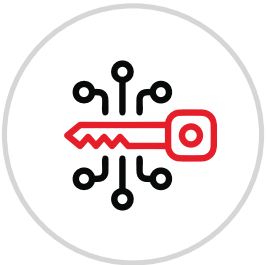
Password Reconciliation & Auto Heal



The process of verifying the passwords of privileged accounts stored in the PAM solution with their actual passwords on the target systems is referred to as password reconciliation in ARCON PAM. Through auto healing, any inconsistencies are automatically identified and corrected, ensuring that the passwords in the PAM solution are accurate and up to date. The solution verifies the passwords of privileged accounts from the target systems regularly and compares them to those stored in the PAM solution. This procedure assists in reducing the risk of unauthorized access or other security breaches caused by outdated or incorrect passwords. Logs on various activities, such as reconciliation status, reason for failure, and success status, are provided.

Just-In-Time Privilege

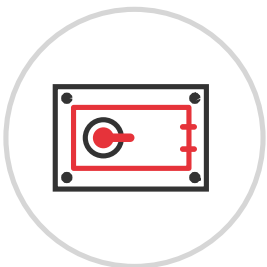
One of the important principles in privileged access management- the principle of “least privileges” can be implemented with ARCON’s JIT privilege capabilities. It ensures that the right person has access to the right systems at the right time. 24*7 or “always on” privileges are too risky. JIT allows users to get temporary access to perform tasks that require elevated privileges without granting them permanent access, lowering the risk of cyber-attacks due to privileged credential misuse. It enables organizations to limit users' privileges to the bare minimum while monitoring and auditing elevated access requests. With JIT approach, access is granted for a limited time and is automatically revoked once the task or operation is completed. This helps to ensure that privileged access is only used when necessary and is not left open for unauthorized access. In ARCON PAM for AWS, for example a user is granted temporary access to an AWS resource such as EC2 instance with the help of Security Token Service (STS), which provides temporary credentials for accessing AWS resources.



Ephemeral Access

This is Just-in-Time privileged interactive access to automatically generate rule and role-based temporary access rights. Amazon Web Services (AWS) Console or Command Line Interface (CLI) component that interacts with AWS Secure Token Service (STS) and allows an administrator to customize accounts with unique AWS roles. When a user logs in to the AWS management console, they are assigned to a particular AWS position and regulation, and they can only execute approved operations on the AWS network.

My Vault



My Vault provides a centralized repository where all critical or privileged data for an organization can be securely stored using advanced encryptions algorithms and role-based access controls. Privileged users can upload files encrypted and stored in a centralized/ quarantined repository. My Vault also allows users to transfer files from the centralized repository to the target servers without requiring them to log in to individual servers.

Users can upload, download, view, and delete files from the vault in the same way that they would on a regular drive. Files are stored on the centralized server, which the Administrator configures, and all Secrets added or uploaded are stored in the database in an encrypted format. Users can share documents, spreadsheets, images, certificates, SSH Keys, directly with other My Vault users or with the public via a link without sending them via email or printing them.

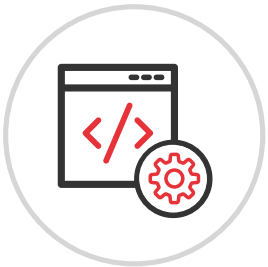
My Vault is protected by multiple layers of security, including authentication, authorization, access control, and encryption. These layers make the solution secure for use by any kind of organization in terms of the size, from small to enterprise.

Application to Application Password Management

When the password of any target device is rotated and if it has any dependencies on other applications then it is important that when the password at the source is changed then its footprints on different applications are also handled upon. With ARCON PAM, the Application-to-Application password change process can be configured to trigger credentials change automatically when the target device password is rotated, ensuring that the users can continue to access the required resources without interruption as the passwords at other applications are synced & propagated. This adds an extra layer of security and ensures that sensitive application passwords are always current and secure.

Application Gateway Server

The Application Gateway Server is ARCON PAM's vital component that allows secure access to applications running on a target system. It serves as a bridge between the user and the applications of the target system. Users can access applications through the Application Gateway Server without having direct access to the target system or its applications. The solution offers secure access via various protocols such as HTTP/HTTPS, RDP, SSH, Telnet, and others. It also provides session recording and monitoring, allowing administrators to keep track of user activity and, if necessary, take appropriate action. ARCON Application Gateway Server streams the application's user interfaces in real time to the end-user device. ARCON Application Gateway Server's streaming technology ensures that the application's performance is unaffected, and that the end-user experience is smooth and seamless. The gateway server also secures application access, preventing unauthorized access and protecting sensitive data.



Privileged Task Automation (Script Manager)

ARCON Privileged Access Management (PAM) includes Privileged Task Automation, which allows administrators to create, store, and manage scripts that can be executed on remote machines. It aids in the automation of repetitive tasks, the reduction of human error, and the improvement of operational efficiency.

Privileged Task Automation allows organizations to easily manage and execute scripts with a few clicks, reducing manual intervention and streamlining task execution.

Datawatch

Datawatch is an ARCON PAM feature that assists organizations in monitoring, detecting, and alerting on anomalous database activities. It collects and analyses database logs in order to identify potential security threats or compliance violations.Users can login to any database application, for example SSMS, etc. using ARCON PAM credentials without logging into ARCON PAM.

TDS Proxy is an ARCON Datawatch component used to monitor access to databases. It connects the SQL Server to the Datawatch Collector. All SQL queries and transactions executed on the SQL Server database are captured by the Proxy and sent to the PAM Vault.

Digital Vault

ARCON | PAM Secrets Management leverages REST-based APIs to authenticate and provide controlled access to the non-human identities, third-party applications, or custom-developed applications to fetch secrets. With the tremendous use of APIs to aid applications access PAM entitlement, various authentication methods have been developed over the period. ARCON PAM has meticulously examined these methods and has integrated with most of the authentication methods to adapt to the evolution of Digital Vault over time.

Development and Operations (DevOps) is one area in IT security where ARCON | PAM acts as a trusted vanguard to ensure controlled access and protect scripts and other embedded secrets throughout the DevOps pipeline.

At a time when IT enterprises are in pursuit of automation through Continuous Improvement and Continuous Development (CI/ CDs) for faster build and release. ARCON | Privileged Access Management enables seamless DevOps journey by providing an additional security layer for enterprise DevOps pipeline.

Digital Vault offers Software Development Kits (SDKs) and Plugins that can be integrated with a variety of third-party tools to enhance the solution's capabilities. The SDKs enable the development of customized applications that interact with the Digital Vault solution, allowing for seamless integration with existing workflows and processes. The plugins can be used to extend Digital Vault's functionality to support additional use cases and workflows. ARCON Digital Vault assists organizations in developing a more comprehensive and flexible solution that can adapt to their specific needs by providing these SDKs and plugins.

Global Remote Access

Global Remote Access (GRA) is a remote access tool that improves end-user experience by reducing unproductive time spent in seeking approvals for critical accesses for days. It automates IT processes and has the ability of authorized users to remotely access and manage unattended devices such as servers, desktops, and laptops without the need for any approvals. For Remote Technical Support, an end-user must manually grant access to another user or support personnel to access their system or resources. ARCON Global Remote Access allows secure authentication for convenient resource access, and it also allows IT teams to create and manage remote access support tickets. An authorized administrator can grant or deny user's requests for elevated access privileges. GRA enables users to securely transfer files between remote devices without relying on third-party file sharing services or email attachments. With Secure File Transfer, users can easily and securely transfer files such as documents, images, videos, and others between remote devices through an encrypted connection.

Identity Governance (User Access Governance)

Identity governance (IG) refers to the policies, procedures, and technologies that are used to manage digital identities and their access to resources. IG assists organizations in ensuring that the right people have the right level of access to the right resources at the right time, while also ensuring regulatory compliance and mitigating risk. Identity governance includes the entire identity lifecycle, including identity creation, management, and deletion, as well as ongoing monitoring, review, and certification of access rights to ensure that they are appropriate and up to date. Additionally, Identity Governance also has a Challenge Phase where the user can view the asset details that the reviewer has preserved/revoked. In the case of revoked assets, the user will be able to challenge the reviewer by presenting a compelling reason for changing their review decision.

Features for
IT Efficiency

Single Sign-On

IT infrastructure comprises multiple layers of devices or endpoints to access systems, which in turn leads to multiple system admins. Therein lies a problem. Multiple system admins mean multiple user-ids, multiple passwords, and multiple approval processes. The Single Sign-On feature allows organizations to overcome this challenge.

ARCON offers the most advanced SSO for almost all conventional IT devices with more than 200+ plug-n-play connectors. This covers a range of devices including Windows, Unix, Databases (Toad, SQL+, SQL Developer etc.), Network Devices, VMWare, Hyper-V, Peripheral devices consoles, and Web Applications.

It even allows seamless access across technologies with just one click. It even prevents possible abuse of privileged accounts while implementing the principle of least privilege.

Auto-discovery

Auto Discovery in ARCON PAM refers to the automatic detection and inventory of IT assets and resources across the organization's IT infrastructure, such as servers, network devices, databases, applications, and user accounts.

This function scans the network for privileged accounts associated with devices and applications. It then generates a detailed inventory of these accounts, giving organizations complete visibility into all privileged accounts in their environment. This feature saves organizations time and effort spent manually identifying and managing privileged accounts, lowering the risk of cyber threats caused by overlooked or unsecured privileged accounts.

Auto Onboarding

Auto onboarding allows administrators to seamlessly add new server groups, user accounts with associated privileges to map new users onboarded on ARCON | PAM. It auto onboard users and assets and map them to appropriate rules (based on roles).

ARCON | PAM supports Auto-Onboarding from cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) to ensure that users and assets are discovered and managed centrally managed through the portal. This feature enables organizations to discover, onboard, and secure the access through cloud infrastructure.

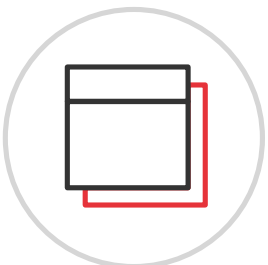
Offline Vault

ARCON|Offline Vault enables remote users not connected to PAM to conduct offline sessions. The service requests must be approved before performing their required activities offline. The activities of these users are audited. Once the PAM server is available, these offline activities are synchronized back to the ARCON PAM Application using the offline sync service.

Virtual Grouping

Managing various systems by different teams and yet retaining control within the teams is a complex task. ARCON | PAM provides a dynamic group setting with one too many relationships and virtual grouping. Thus, one can create functional groups of various systems and help in facilitating relationships, responsibilities, and accountabilities. This feature caters very well to dynamically changing organizational structures, roles, responsibilities and even allows managing multiple subsidiaries and companies.

Tag Management is a feature that allows users to effectively manage privileged assets. Users can categorize, label, and classify privileged assets based on criteria such as location, ownership, sensitivity, and function. Administrators can use this categorization to group resources based on business objectives and ensure that access is controlled and audited in accordance with policies and regulations.

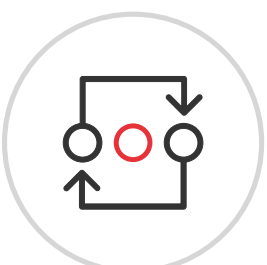


Workspace App

The multi-tab feature allows users/administrators to open multiple sessions in different tabs in the same window and allow them to switch between sessions as required. Multi-tab feature is supported by SSH and RDP service types. Multiple service sessions if opened in a tabbed manner in a single window makes it easier for the user to toggle between services and control all user sessions centrally.

Behaviour Analytics (also known as Knight Analytics)

Knight Analytics is a deep-learning threat detection system developed by ARCON | PAM. This AI-based technology detects, predicts, and displays anomalies in the logged data. It uses machine learning algorithms that learn each user's behavior based on their historic data and predicts risk based on the activities. It displays concerning users, sessions, commands, and processes that one should be aware of as the most important security issues with respect to users, sessions, commands, and processes that one should be aware of so that one can make better-informed business decisions. Alerts are received based on the risky entities, the one with the greatest potential risk level /risk score.



Connector Framework

With the increasing demand for new IT mechanisms rising in an organization, the protection of the systems by integrating them with ARCON | PAM becomes radical. ARCON Connector Framework automates the process of creating connectors by eliminating the need for manual data collection. It also simplifies the process of provisioning any new application which is not available in PAM.

Robotic Process Automation (RPA) is the process of automating mundane tasks with ease, efficiency, and accuracy. ARCON PAM users can integrate with various automation solutions. ARCON | PAM offers a provision to customize steps for the end-users for any SSO activity.

It could be image-based control recognition, shortcut keys, and Control ID. The RPA technology can even ensure all use cases of the connectors are fulfilled.

Incident Management

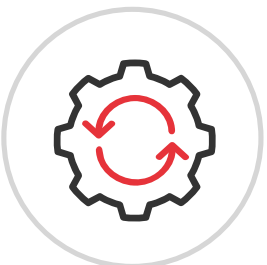
Incident response mechanisms are given utmost importance today. It is crucial to respond to applicable incident data in the shortest time to avoid any major loss. Traditionally, after the incident, the IT teams need the ability to analyze the reasons, the activities post incident and identification of areas for better responses.

If this process is automated, then there can be synergies across the Incident response team and it can save lots of valuable time. With Incident Management feature, a privileged user is able to identify and raise an incident for any activity that looks to be suspicious.

One Admin Control

No matter how big your enterprise's IT infrastructure, each and every access to critical systems is made through one ADMIN console. The secure gateway server provides a centralized control point through which all network connections and traffic is routed for management and monitoring.

Unified admin console to manage entities and access to the target systems/applications. Authorization ensures the implementation of an access control framework around people and policies. This way, the privileged access is granted only on a "need-to-know" and "need-to-do" basis, the foundation for robust identity and access control management.



Workflow Management

No more tedious and long approval process. The Workflow matrix makes administrators' lives easy. It enables configure the approval process for privileged users, user-groups, and service groups. Workflows can be set for admin activities/transactions as well as for user access requests. Service Access and Service Password request workflow mechanism speed up the process of assigning target servers to privileged users.

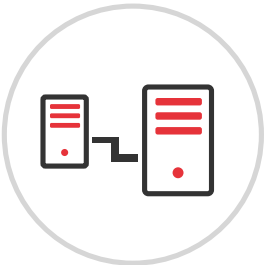
Privileged Elevation and Delegation Management (PEDM)

Privileged Elevation and Delegation is a feature in ARCON PAM that allows authorized users to temporarily elevate their privileges to perform a specific task or execute a command that requires higher privileges than they currently have. It provides a secure mechanism for granting privileged accounts temporary elevated access without exposing sensitive credentials to unauthorized users. This is useful in situations where users need to perform specific tasks or run specific applications that require higher privileges but are not always authorized to do so. This feature ensures that privileged access is granted only to authorized users for the time required to complete the required task, thereby improving the organization's security posture.

Browser Plugin

This is a browser-independent extension available for all platforms that offers a point solution for shielding all of the classified secrets and confidential assets for your organization at a single location. With the Browser Plugin, users can automatically sign in to a range of applications that are offered by ARCON | PAM without entering the credentials manually or even remembering them each time they access the applications directly from any browser available on their desktop.

AD Bridging



The main purpose of AD Bridging is to manage and connect to di erent operating systems within the same network infrastructure from Microsoft Active Directory (MAD) console to connect data. MAD can accept natively ordinary and non-privileged accounts from non-Windows machines.

AD Bridging tool in ARCON | PAM allows organizations to use Microsoft AD as their authoritative source of identity, while extending it to the systems, apps, and protocols not natively managed by Active Directory. Once the primary users are authenticated against AD Bridging, it supports Linux and Unix Operating Systems.

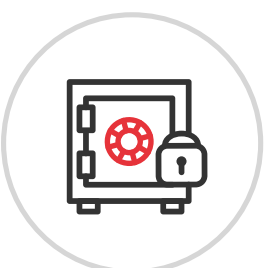
Integration

ARCON | PAM provides seamless integrations with a variety of tools from SIEM, ITSM, RPA, DevOps CI/CD, IDAM, Automation Solutions, Containers and more. Some of the tools that can be integrated with ARCON are Symantec, RSA, Arcsight, Rapid7, BMC Remedy, Precision, ServiceNow, Nessus Manager, Tenable.io/Tenable.sc, Qualys, Ansible, Jenkins, Chef, Kubernetes, Red Hat OpenShift, AWS Elastic Container Service (ECS), Microsoft AD, Azure Ad, G-Suite, AWS IAM, Okta, Sailpoint, 1Kosmos and many more.

vRA provides operations management across physical, virtual and cloud environments. vRA(VMware vRealize Automation) automation can be leveraged to perform automation for Service provisioning in PAM when a new VM is created.

CLI Proxy

The CLI (Command Line Interface) Proxy component in ARCON PAM allows administrators to manage and monitor remote devices and systems without logging on to the PAM console or web interfaces. It serves as an intermediary between the user and the target machine, allowing the user to remotely execute commands on the target device without logging into the PAM portal. Administrators can use CLI Proxy to execute commands, scripts, and other operations on remote machines from a centralized location without physically accessing them. This not only saves time and effort, but it also improves security by lowering the risk of unauthorized access or system changes. CLI Proxy is useful in situations where administrators can use their own set of CLI tools, for example Putty, MobaXTerm, SecureCRT, for RPA processes.



Vault Broker Suite

Vault Broker Suite is designed for human or non-human identities that require privileged passwords as well as channels to connect to the various systems. It is required only if the target applications are not able to make a direct connection to the target systems.

Instead of forcing the client to create trust with ARCON | PAM Vault, there are modules to transfer the authenticated connection to the client, eliminating the need for the client to fetch credentials. The Vault Broker not only can securely connect to the ARCON | PAM Vault but also third-party vaults.

Features for

Compliance & Reporting

Customized 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 activities 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. It helps them to make better IT privileged user decision making. The solution enables managers and auditors to assess the organization's regulatory compliance status at any given time.

Audit Trails - Text & Video Logs

ARCON | PAM proactively secures all databases and applications as every command/query executed by end-users is captured for a security assessment. This way, the Security and Risk Assessment team seamlessly manages the lifecycle of privileged accounts as every activity performed by privileged users is captured in both video and text format.

Analytics Reporting Tool (also known as Spection)

The tool leverages the solution's analytics platform to generate dynamic reports with statistical as well as the graphical representation.Spection gives freedom to choose a report and view it as per their individual requirement. All the necessary entities and elements of a report are filtered and arranged to generate a dynamic report with the help of Spection.

Compliance - Regulatory Standards

ARCON | PAM enables organizations in fulfilling regulatory requirements from a single platform. Guidelines provided by European Union (GDPR), PCI-DSS, SWIFT, ISO-27001, BASELIII, HIPAA, SOX etc. have made it mandatory for organizations to have a necessary IT security infrastructure in place, which would safeguard privileged accounts from unauthorized activities.

arcon

ARCON | PAM

Benefits at a glance

- It helps to meet with the regulatory mandates and IT Standards
- Ensures privileged access to target systems only on a 'need-to-know' and 'need-to-do' basis
- Enhances overall IT efficiency and ensures security of confidential data
- Highly mature Password Vault to randomize privileged passwords, on-scale
- Secrets Management for DevOps and CI/CDs Environments
- Offers the deepest level of granular controls to enforce the least privilege principle
- Provides Just-in-time Privileges (JIT) to target devices
- Offers Privilege Elevation & Delegation Management (PEDM) capabilities
- Support for modern-day use-cases: Cloud Access, DevOps, API workloads, Bots
- Global Secure Remote Access for addressing the 'New-Normal' access control challenges
- A large connector framework to support both third-party tool integrations and quick deployments
- Leverages AI/ML for advanced threats analytics
- Highly scalable & customizable
- Privileged Session Management with robust Multi-Factor Authentication, Centralized Dashboarding, Session Monitoring and Reporting

arcon

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.