arcon

Predict | Protect | Prevent

Privileged Access Management

Introduction

Privileged Access Management (PAM) is one of the most important areas in Information Security. As the term suggests, privileged access is granted to privileged users.The privileged users have elevated access rights to business-critical applications, databases, cloud-resources, DevOps, CI/CDs environments among other highly sensitive data-assets.

Thus, managing, monitoring and controlling the privileged access is extremely important. Misuse or abuse of trusted privileges is one of the biggest sources of data breaches and abuse of sensitive information. A robust privileged access management is essential to thwart insider threats, third-party risks and advanced cyber-attacks. Privileged Access Management practice helps to ensure that any unauthorized access to target systems is denied.

Besides, Privileged Access Management is essential from the compliance perspective. A host of IT standards such as PCI-DSS, HIPAA, ISO 27001, and regulations (GDPR) among many other local regulations as mandated by governments and central banks explicitly ask for role and rule-based access, Multi-factor authentication (MFA), password vaulting, etc. to protect data. The solution offers all the necessary safeguards.

However, the level of complexities in managing privileged users is increasing; so is the level of the privileged access control. Many global organizations have distributed data center environments. More and more organizations are adopting cloud-computing. IT developers have privileges to access DevOps tool chains. Furthermore, the pandemic and its implications have meant that most of the workforce access systems remotely.

All these use-cases have necessitated granular control over privileged users along with a strong validation mechanism.

Against this backdrop and the proliferation of privileged users, a robust Privileged Access Management is a must to ensure authorized and controlled access to systems.

ARCON | PAM provides the capability to address an enterprise's privileged access use-case challenges

Built to address the evolving privileged access use-case challenges, ARCON | PAM offers best-in-class access control features. A feature-rich solution, ARCON | PAM offers an IT security team with the deepest level ofgranular controls and Just-in-time (JIT) privileged access to enforce the principle of least privilege in any ITenvironment.

Trusted by more than 1000 global organizations, spanning wide-ranging industries, the enterprise-grade solution offers a best-fit architecture to ensure scalability, IT efficiency and privileged access security including compliance.

Features for

Security, Monitoring & Governance

Fine-Grained Access Control

ARCON has a unique technology framework that provides granular access control for privileged users, despite being natively super users. It is not possible to restrict their access to any system.

This is possible for several technologies i.e operating systems, databases, network and security devices etc. Fine-grained access control helps organizations to protect their systems from unauthorized access and unintentional errors, if any. It allows to restrict and control privileged users through a rule and role-based centralized policy.

The feature provides the IT risk managers command restricting and filtering capabilities to ensure secure, authorized and controlled access to target systems. It minimizes the risk surface by providing deepest levels of granular control over privileged users.

Password Vaulting

There are many privileged users within any IT setup with shared privileged passwords. This practice of shared passwords makes systems and applications vulnerable to misuse or abuse. Moreover, it is extremely difficult to establish manual control over the password change process.

ARCON | PAM provides a highly mature password vault that generates strong and dynamic passwords and the engine can automatically change passwords for several devices or systems at one go. The passwords are then stored in a highly secured electronic vault. The storage methodology is proprietary and is highly secured by several layers of protection that ensures a virtual fortress.

The electronic vault integrated with ARCON | PAM workflow provides authorized access to these passwords. Password Vault enables enterprises to handle complex password changes including evolving regulatory mandates.

SSH Keys Management

SSH keys reinforce an enterprise's authentication control management. SSH keys are valuable credentials to access privileged accounts. It provides an additional access control security layer. SSH keys are a reliable and secure alternative to Passwords as brute-forcing a password-protected account is possible with modern processing power combined with automated scripts. SSH key pairs are two cryptographically secure keys that can be used to authenticate a client to an SSH server.

Multi-factor Authentication

Privileged account access requires well-established identity references (validation) for users accessing critical IT components. Multi-factor authentication (MFA) provides a robust validation mechanism. The solution’s MFA functionality acts as a strategic entry point to identity management systems and helps in managing system-based users.

ARCON offers native software-based One-Time-Password (OTP) validation to begin a privileged session and the tool seamlessly integrates with disparate third-party authentication solutions such as Gemalto, RSA, Vasco, 3M, Precision, SafeNet and Safran.

Session Monitoring

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

Password Reconciliation

With ARCON's Password Reconciliation, day-to-day administrative tasks become easy. Once the latest credentials from ARCON | PAM, i.e IP Address, Port, Username and Password for a particular service is received, it connects to the target device automatically using those credentials.

Once successfully connected, it gets updated into ARCON | PAM states that the particular service is live and has an updated password. All the status of success and failure are updated in the Service Reconcile Status Report. This automation helps in enhancing the best-privileged practices.

Just-In-Time Privilege

ARCON | PAM Just-In-Time Privilege is a powerful tool that ensures that any privileged access is allowed according to an approval workflow while adhering to the security. With JIT privilege practice, the enterprise IT risk team can ensure all users act as standard users, and not as privileged users. After any request is raised, administrators allow privileged rights to any user to perform a definite task at a specified time.

ARCON | PAM JIT privilege removes standing privilege by limiting access to systems/ applications and the count of administrative/ operational staff. It even limits access at a granular level and denies full-time access to internal systems/ applications.

My Vault

My Vault is an integral part of an ARCON | PAM solution that secures an organization's classified and confidential documents by allowing limited sharing of the confidential data assets.

To cater to this requirement, My Vault not only satisfies it successfully but also takes care of the secrets of all the servers that are not rotated through the PAM solution. Thus My Vault and PAM together allow seamless management of all privileged servers, assets and secrets in an organization.

App to App Password Management

App to App Password Management of ARCON | PAM manages the passwords for an application through a single terminal in the IT infrastructure. This is an automated process where the password change is managed and monitored by giving the required details of the servers, the IP addresses and the new passwords.

It is a smooth process that synchronizes the changes across the network to prevent service disruptions. All the changes are examined in the configuration file before and after the task.

Application Gateway Server

ARCON Application Gateway server (AGW) can stop execution of attacks on enterprise's most sensitive IT infrastructure. It uses the network overlays, network encryption, software-defined perimeter and host based agents to establish a secure VPN-less connection. The tool suffices Zero Trust Network Access (ZTNA) framework. Access to systems is based on 'identity' along with other attributes and contexts such as IP address, geo-location, devices used, time and date. Overall operational efficiency is maximized by AGW along with robust access monitoring.

Remote Assist

Remote Assist helps system administrators to remotely access and troubleshoot end devices anywhere on the globe. It helps to resolve help-desk tickets, or desktop issues instantly. This secure remote desktop solution offers granular control over your network and allows you to connect to specific users within or outside the enterprise network, while ensuring IT security, and security compliance.

Guard

ARCON | Guard application is an SSH server-based utility that is installed centrally on the server. It can be integrated with ARCON | PAM application for command restriction and elevation. It restricts and elevates all the commands when the guard installed SSH server is accessed through third-party applications.

This is configured to restrict commands and monitor the session even in case of the unavailability of the ARCON | PAM. The file monitoring feature detects when and who made the modifications to critical system configuration files on the server.

Script Manager

It helps an end-user to manage and control various scripts of a system and monitor their execution. ARCON | PAM has visualized automation as an important feature for safe IT operational solutions. In line with that, ARCON | PAM Automation Script Manager offers full Role-Based Access Control where automation scripts modification and execution rights can be configured based on the end-users' roles. This way, ARCON | PAM Script Manager helps the Administrators to run scripts and monitor multiple databases continuously.

Datawatch

What would happen if we can track and control database queries and map them back to the privileged session through PAM? Session monitoring might not always be the best way to track commands or queries. ARCON | DataWatch after integrating with PAM, acts as a gateway to all database connections, captures the queries & responses and maps them back to the session.

Smart Session Monitoring

The advanced session monitoring module named Smart Session Monitoring (SSM) helps with fast-track reviews of the videos by highlighting critical events in the media. Also, it seamlessly monitors activities performed on the server such as user activities, mouse-clicks, optical character recognition, keystrokes and processes launched.

Digital Vault - Secrets Management

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.

Digital Vault - DevOps

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.

Global Remote Access Solution

This is the most crucial feature launched due to the pandemic. ARCON Global Remote Access Solution (GRAS) offers remote users to establish a remote connection to their assigned desktop or laptop from outside the infrastructure environment securely. Also, the end-users can address the downtime issues or troubleshoot the machine in a controlled environment without the necessity to install and configure the costly VPNs. This solution is simple to use and is a cloud-native application.

User Access Review

IT helps the IT administrators to review the service access granted to the users at regular intervals. The admins can define a new user access review process, wherein the review process is initialized through an email for approval.

The process of setting the scheduler has a start date and the number of due days of the approver can be reviewed before being set. On that particular day, the approver receives an email that is valid for the number of days set by the Admin. Even the admins can modify the details of configured user access and terminate the access before being initialized.

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.

Features for

IT Efficiency

Auto-discovery

IT infrastructure faces a huge risk in a shared and distributed privileged account environment. It's a big challenge for the security and risk management team to identify and track the ownership of privileges.

To overcome this challenge, ARCON auto-discovery enables the risks management team to discover shared accounts, software and service accounts across the IT infrastructure. Identification and tracking of privilege ownership mitigate risks associated with the lifecycle of a privileged account.

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.

User Onboarding

User onboarding allows administrators to seamlessly add new server groups, users accounts with associated privileges to map new users onboarded on ARCON | PAM. It enables administrators to auto-provision and deprovision users or devices by interacting with active directory.
With user onboarding, organizations can ensure that all information collected while onboarding stays confidential and locked in a virtual database and out of reach from any kind of physical or unauthorized access.

Single Sign-On

IT infrastructure comprises multiple layers of devices or endpoints to access systems, which in turn leads to multiple sys-admins. Therein lies a problem. Multiple sys-admins mean multiple user-ids, multiple passwords and multiple approval processes.

The Single Sign-On feature allows us to overcome this challenge. It relieves the difficulty for sys-admins from managing multiple passwords on different devices such as networking devices, databases, etc. When sys-admins use connectors to connect all these components, then it is easier and simpler for the admin to use single- sign-on without having to remember individual user-id and password.

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.

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.

ARCON PAM provides a unified policy engine to offer a rule and role-based restricted privileged access to target systems. 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 to configure the approval process for privileged users, user-groups and service groups. Service and password request workflow mechanism speeds-up the process of assigning target servers to privileged users.

Privileged Elevation and Delegation Management (PEDM)

While ARCON | PAM allows an enterprise to build a security layer around privileged accounts by granting access rights to full administrative users based only on predefined access control policy, Privileged Elevation and Delegation Management (PEDM) supplements privileged user management by controlling and monitoring non-admin user activities that require temporary privileged access to the systems.

PEDM essentially discards unnecessary escalation of privileged accounts. An excessive number of privileged accounts, especially in a distributed IT environment, increase potential threats to sensitive information. The tool is an extension to a granular control approach that enables an enterprise to mitigate risks by granting temporary administration rights only on a "need-to-know" and "need- to-do" basis.

Access to critical components such as applications, databases, cloud services is granted only aGer a valid automated approval process. Access rights assigned to critical systems are automatically terminated aGer the conclusion of "temporary privilege" activities. Further, just like every privileged session activity is documented for audit purposes, the audit trail of PEDM initiated sessions can also be maintained through comprehensive reporting. Hence, it allows an enterprise to gain operational flexibility while ensuring compliance and a robust security framework.

AD Bridging

The main purpose of AD Bridging is to manage and connect to different 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.

Session Management (also known as Multi-tab)

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.

Desk Insight

Sometimes, it becomes a challenge for IT help desk to attend requests from one desktop to the other. ARCON's Desk Insight is an effective tool that enables an administrator to manage requests from any on-boarded desktop in the network. It also allows a help desk engineer to troubleshoot a machine without moving from one desktop to the other. Desk Insight also enables end users to elevate admins rights, privileges, change passwords, and access related tasks in a controlled environment.

Behaviour Analytics (also known as Knight Analytics)

Knight Analytics is a deep learning threat detection system developed by ARCON | PAM. This AI-based technology is used to detect, predict and display anomalies in the logged data.

It uses machine learning algorithms that learn each user's behaviour based on their historic data and predicts risk on the basis of the activities. There are six different graphs that display the risk percentage to the administrators. These are User Analytics, Service Analytics, User Group Analytics, Service Group Analytics, Group-wise User Analytics, and Group-wise Service Analytics.

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.

Robotic Process Automation (RPA)

Doing regular mundane IT tasks is always a dislike for all IT users. Robotic Process Automation (RPA) helps to automate these tasks with ease, efficiency and accuracy. 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.

vRA

With the burgeoning cloud services and technological advances such as VMWare, organizations have the proclivity towards increasing agility, productivity and efficiency through cloud automation, by reducing the complexity of their IT environment, streamlining IT processes and delivering a DevOps-ready automation platform.

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. ARCON | PAM provides integration with automation solutions like vRA(VMware vRealize Automation) to enable onboarding and de-boarding of privileged accounts as well as devices/ systems.

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.

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.

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.

Integrations

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.

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

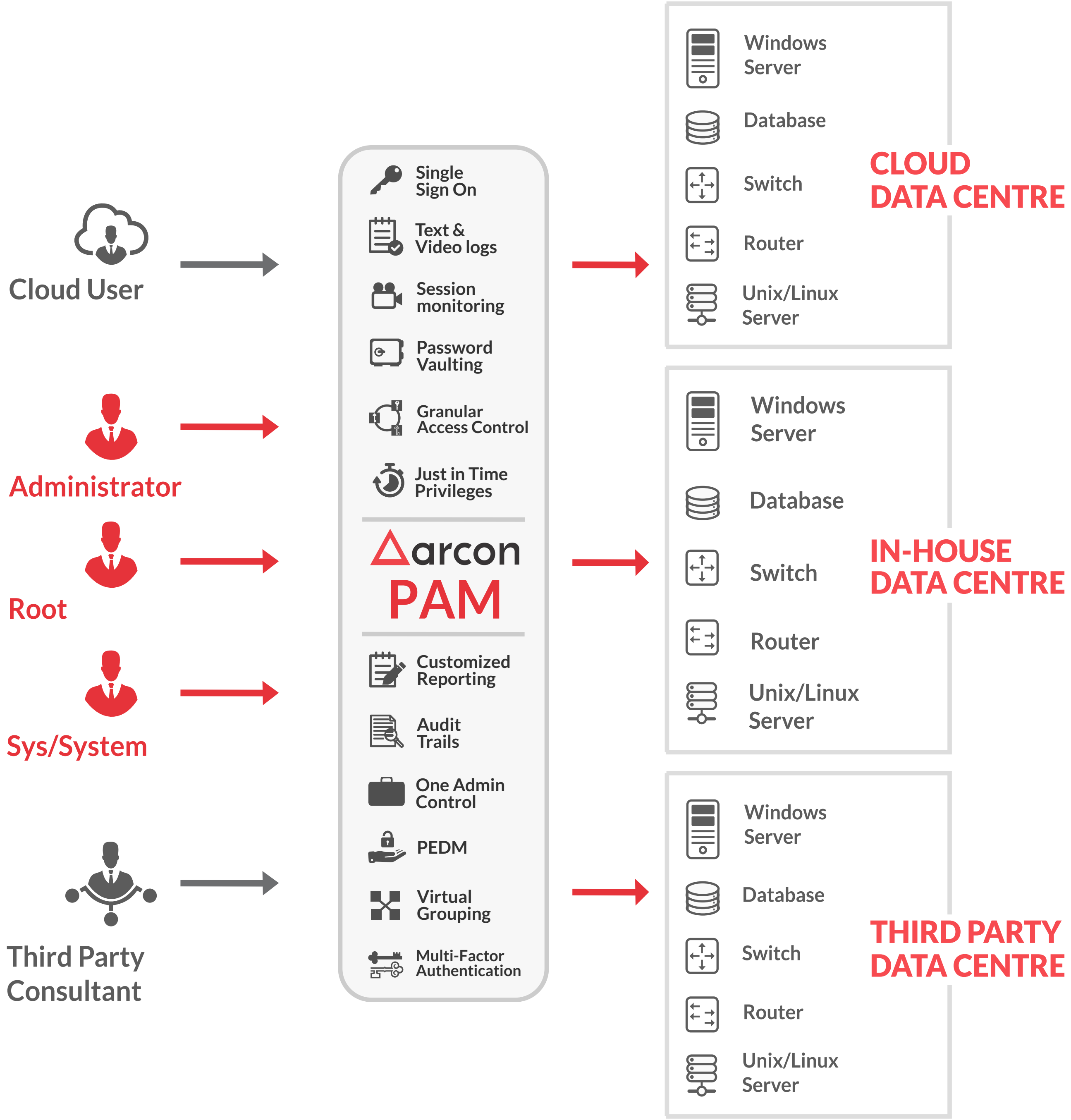
ARCON | PAM enables organizations in fulfilling regulatory requirements from a single platform. Guidelines provided by European Union (GDPR), PCI-DSS, SWIFT, ISO-27001, BASELIII, HIPAA, SOX etc. have made it mandatory for organizations to have a necessary IT security infrastructure in place, which would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

ARCON | PAM

key-points 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

Product Atchitecture



Cloud User

Administrator

Root

Sys/System

Third Party Consultant

Single Sign On

Text & Video logs

Session monitoring

Password Vaulting

Granular Access Control

Just in Time Privileges

arcon PAM

Customized Reporting

Audit Trails

One Admin Control

PEDM

Virtual Grouping

Multi-Factor Authentication

CLOUD DATA CENTRE

Windows Server

Database

Switch

Router

Unix/Linux Server

IN-HOUSE DATA CENTRE

Windows Server

Database

Switch

Router

Unix/Linux Server

THIRD PARTY DATA CENTRE

Windows Server

Database

Switch

Router

Unix/Linux Server

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 enterpris e 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