Arcon

Privileged Access Management

Introduction

ARCON | Privileged Access Management (PAM) redefines the essence of information security with its path-breaking risk-control solution sought by most security professionals in the genre of digitization.

Why do organizations require Privileged Access Management?

The IT infrastructure of any organization is never static. As it grows, the number of applications, servers, cloud resources, amongst several other critical systems also increases, leading to proliferation of privileged identities. These identities are authorized with elevated privileges to access target systems. Privileged identities are spread across the enterprise, touching every aspect of IT fabric like operating systems, databases, servers and network devices; and hence are in position to access highly-classified data.

Due to their intrinsic significance in the whole IT fabric, privileged identities are always vulnerable to misuse by malicious insiders, disgruntled employees or compromised third-party elements. Several research reports show that about 75% of data breach incidents happen due to compromise of privileged credentials.

ARCON's Privileged Access Management (PAM) is a best-in-class solution that reinforces the privileged access control mechanism. The solution offers best privilege account management practices and lays the foundation of robust identity and access management. It offers the deepest level of granular level control over privileged users along with robust multi-factor authentication and password vaulting to secure enterprise datacenter. Trusted by 500+ enterprises worldwide, ARCON | Privileged Access Management offers a best-fit architecture ensuring scalability for an enterprise. It seamlessly supports cloud platforms.

ARCON | PAM offers a fine balance between security, compliance and business efficiency.

Today's CIOs search for a comprehensive security solution which offers business efficiency, robust security control mechanism and default security compliance structure. Any management expects a decent return on investment (ROI) for every budget they allot. ARCON | PAM's seamless controlling, monitoring and securing of privileged accounts not only protects data assets from malicious insiders and third-parties but also ensures business continuity in truer sense. It offers all requirements under one roof and strikes a fine balance between IT operational efficiency, security and compliance.
Let us find out how the features of ARCON | PAM can help organizations predict, protect and prevent unauthorized access in the enterprise network.

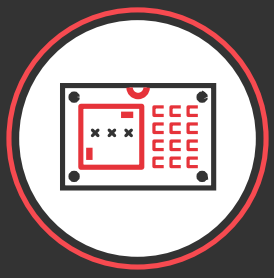
Security

Fine Grained Access Control

ARCON has a unique technology framework which provides granular access control for privilege users, in spite of 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 restricting and controlling privileged users through a rule and role based centralized policy. The functionality provides the IT risk managers command restricting and filtering capabilities for ensuring secure, authorized and controlled access to target systems. It minimizes the risk surface by providing deepest levels of granular control over data controllers and data processors.

Password Vaulting

There are many privilege users within any IT setup and they are shared among multiple users which makes them vulnerable to misuse. It is extremely difficult to establish a manual control around password change process. In addition, the password safety is a big challenge. ARCON provides a highly mature password vault which generates strong and dynamic passwords and the engine can automatically change passwords for several devices or systems at one go. The passwords are 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 and dynamic password changes to meet the regulatory mandates.



SSH Keys

SSH keys reinforce an enterprise's authentication control management. SSH keys are valuable credentials to access privileged accounts. It provides additional access control security layer. SSH keys are reliable and secure alternative to Passwords as the 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 a 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 enables IT security team to spot any suspicious activity around privileged account. Live Dashboard ensures that all critical activities performed by administrators across the IT infrastructure are viewed in real-time.

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 mitigates risks associated with the lifecycle of a privilege account.

Password Reconciliation

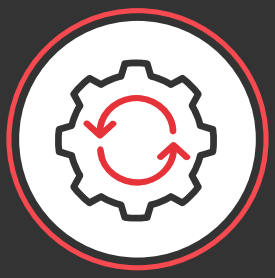
With ARCON's Password Reconciliation, day-to-day administrative tasks become easy. Once the latest credentials from ARCON | PAM, i.e IP Address, Port, Username and Password for a particular service is received, it connects to the target device automatically using those credentials. Once successfully connected, it gets updated into ARCON | PAM stating that the particular service is live and have updated password. All the status of success and failure are updated in Service Reconcile Status Report. This automation helps in enhancing the best privileged practices.

arcon

Efficiency

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 to 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.



Workflow Management

No more tedious and long approval process. 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. Excessive number of privileged accounts, especially in a distributed IT environment, increase potential threats to sensitive information. The tool is an extension to granular control approach that enables an enterprise to mitigate risks by granting temporary administration rights only on "need-to-know" and "need- to-do" basis. Access to critical components such as applications, databases, and cloud services is granted only after a valid automated approval process. Access rights assigned to critical systems are automatically terminated after the conclusion of "temporary privilege" activities. Further, just like every privileged session activity is documented for audit purpose, audit trail of PEDM initiated session can also be maintained through a comprehensive reporting. Hence, it allows an enterprise to gain operational flexibility while ensuring compliance and a robust security framework.

arcon

AD Bridging

Active Directory Bridging is a bridging between Linux machine and Windows AD Server. It is a web based application that allows Users (admin/non-admin) to login into LINUX machine using Windows Active Directory. It automates various administrative level tasks such as installing Kerberos, configuring files, and restarting services for updating the configuration. In addition, it also logs activities performed on LINUX machine.

ARCON | PAM offers all the capabilities with Session Manager, Password Manager and Access Manager Modules to transparently connect primary users of their OS exclusively. The users can even authenticate with the help of a single entry even without modifying the configuration of Active Directory (AD).

Single Sign-On

SSO provides one-time administrative access to all underlying applications. IT infrastructure comprises of multiple layers of devices to access systems, which in turn leads to multiple sys-admins. Therein lays a problem. Multiple sys-admins means multiple user-ids, multiple passwords and multiple approval processes. The Single Sign-On feature allows overcoming 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, it makes it 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.

User Onboarding

User onboarding allows administrators to seamlessly add new server groups, users accounts with associated privileges to map new users on boarded on ARCON | PAM. It enables administrators to auto provision and de-provision 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.

One Admin Control

No matter how big is your enterprise's IT infrastructure, each and every access to critical systems is made through one ADMIN console. The secure gateway server provides 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 implementation of access control framework around people and policies. This way, the privileged access is granted only on "need-to-know" and "need-to-do" basis, the foundation for a robust identity and access control management.

arcon

Multi-tab feature

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.

Compliance

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 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.

Text & Video Logs

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

arcon

Conclusion

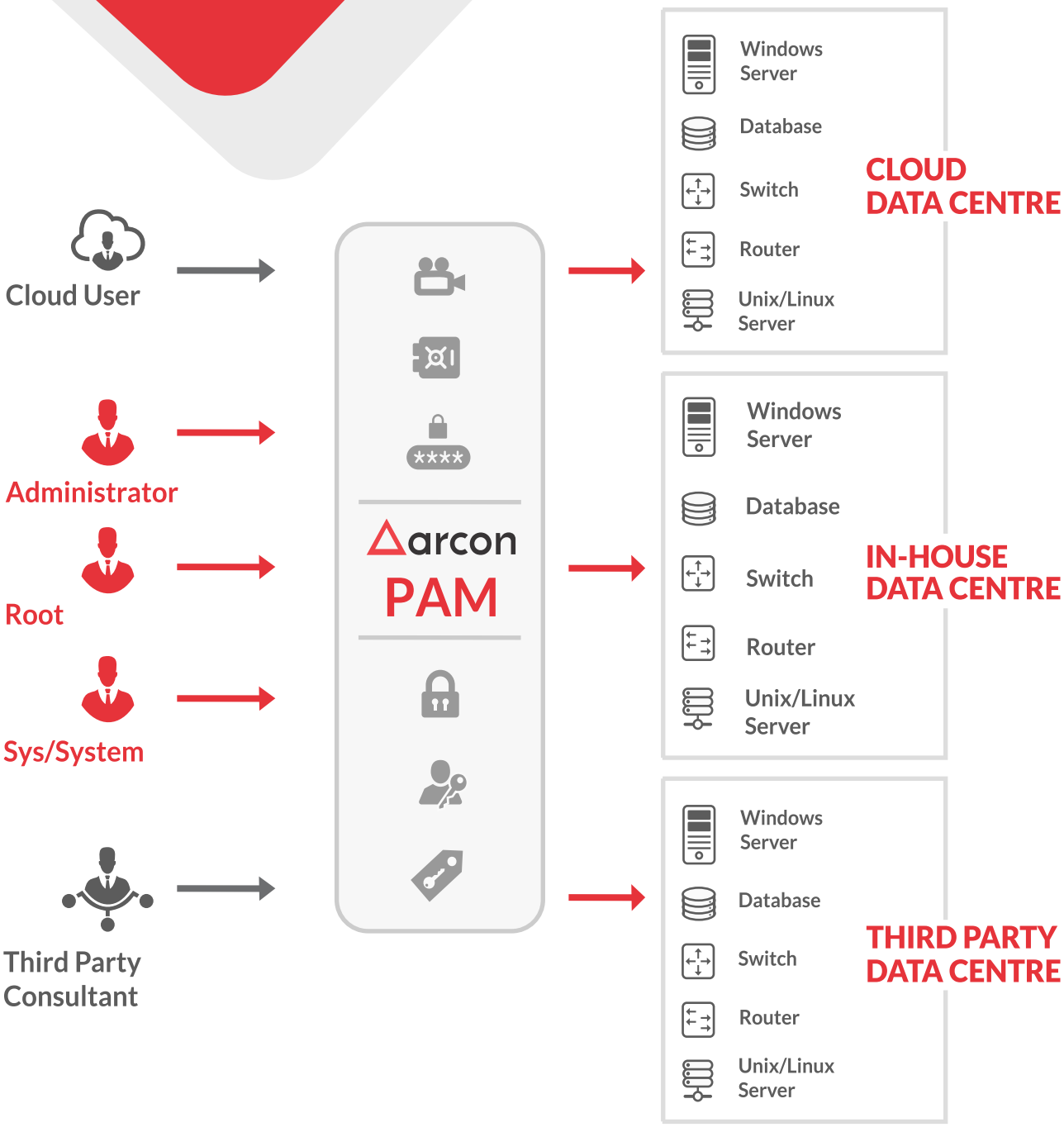
ARCON is a comprehensive solution for Privileged Access Management (PAM), allowing monitoring and controlling security of privileged accounts. In addition, fortifying privileged identities enable firms in fulfilling regulatory requirements from a single platform. Guidelines provided by European Union (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.

This solution provides a layer of abstraction over the underlying IT infrastructure fabric thus enforcing users to logon by using user-id, passwords, and a unique OTP (One Time Password). Not only that, ARCON | Privileged Access Management (PAM) has the ability to provide required access on "need-to-do" basis and can track users' activities distinctly even if they are privileged users.

Privileged Access Management (PAM) solution not only provides a secure umbrella to the underlying IT infrastructure and data but also maintains a complete audit trail of activities linked to privileged accounts. This risk-control tool identifies vulnerabilities and assesses risks at various levels like operating systems, databases and servers.

arcon

Product Architecture



arcon