Arcon

Privileged Access Management

Introduction

ARCON | Privileged Access Management is a pivotal component in the overall Information Security framework

The foundation for a secure identity and access control IT architecture starts with robust ARCON | Privileged Access Management (PAM). ARCON | PAM enables an enterprise IT risk management team to reinforce the security around privileged accounts. It reduces enormous risks emanating from unaccounted and unmonitored privileged accounts, which leads to data breach.

As the term suggests, 'privileged' users have elevated access to sensitive information stored in systems and applications. Hence privileged accounts require utmost security from malicious elements. These elements could be compromised insiders, malicious third parties or organized cybercriminals. The modus operandi is typically the same: stealing or abusing privileged credentials to execute attacks on corporate information. Therefore protecting privileged accounts and privileged credentials is critical to secure sensitive data and business-critical information.

The need for privileged access management primarily arises from ever-growing numbers of privileged accounts in the enterprise IT network. With the digital workplace expanding beyond the normal datacenter perimeter, the threat level has multiplied. Important to note that business-critical information and confidential data is typically managed in shared and distributed environments. These data assets could be stored in databases, servers, along with a host of resources such as service and application accounts, network devices, cloud applications, business-critical applications like ERM, CRM, HR applications, DevOps toolchains and virtualization… not to be left out- social media accounts. Misuse of one privileged account could bring down the entire IT infrastructure to a standstill. Therefore, mitigating risks associated with privileged accounts such as unauthorized access to target systems and applications along with misuse or abuse of privileged credentials is of paramount importance.

Against this backdrop, it is critical for an enterprise IT security team to have comprehensive security measures in place to protect privileged accounts. ARCON | PAM offers a centralized governing framework to manage, control and monitor all privileged accounts in an underlying ecosystem. The solution provides IT risk management teams with necessary tools to secure and vault privileged passwords whilst ensuring authorized privileged access to critical systems, databases and applications through rule and role-based privilege entitlements. Moreover, ARCON | PAM leverages artificial intelligence (AI) powered machine learning (ML) for predicting risks emanating from anomalous privileged identity profiles. With ARCON | PAM an enterprise IT risk management can build a robust 'Zero Trust' architecture, which is pivotal in the overall Information Security framework.

Five reasons why organizations choose feature-rich ARCON Privileged Access Management

1. Highly scalable and customizable
2. Supports High Availability
3. Largest connector framework, fast deployments cycle and prompt support
4. Supports Multi-tier architecture
5. Seamless Integration

ARCON | Privileged Access Management (PAM) is an enterprise-class solution that strikes a fine balance between IT operational efficiency, security and compliance.

Features of

Security

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 which includes operating systems, databases, network and security devices and applications. 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 governing policy. The functionality provides the IT risk managers with command restricting and filtering capabilities to ensure 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 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 a 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 and dynamic changes including evolving regulatory mandates.

SSH Keys

SSH keys reinforce an enterprise's authentication control management. SSH keys are credentials used 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 Session provides basic auditing and monitoring of privileged activities around the enterprise IT network. The features enablesthe 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.

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 unaccounted privileged accounts.

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, showing that the particular service is live and has an updated password. All the status of success and failure is updated in the Service Reconcile Status Report.

Just-In-Time Privilege

ARCON | PAM Just-In-Time Privileges functionality ensures all users act as standard users, and not as privileged users. The functionality helps to implement the principle of least privilege. With JIT Privileges, an admin can provide access to systems and applications only when the requirement arises. Privileges are elevated for specific tasks on applications and systems. After any request is raised, administrators allow privileged rights to any user to perform a definite task at and for a specified time. ARCON | PAM JIT privileges remove 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 systems/ applications.

My Vault

The tool can be used to securely store files in an encrypted format. It allows a user to share such files leveraging the solution. Users uploading the file can set a time limit after which the file will be deleted automatically. End users with My Vault privileges can access those files just like privileges to any applications

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.

Knight Analytics

Knight Analytics is a deep learning threat detection system introduced 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.

Application Gateway Server

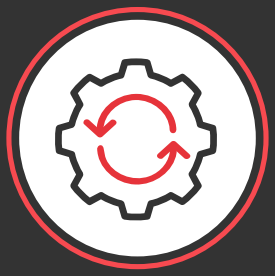
Application Gateway Server (AGW) is the single point of access to the target systems. The secure gateway helps in creating an encrypted tunnel from end-points to the target devices. This is completely integrated within the ARCON | PAM solution and creates an added layer of security for open communication channels.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.

Features of

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 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.



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

Active Directory (AD) Bridging provides authentication to have a single-sign-on, for Linux/Unix users using Windows Active Directory credentials by bridging the machine and AD Server. ARCON | PAM offers all the capabilities with Session Manager, Password Manager and Access Manager Modules to transparently connect primary users to their OS exclusively.

Single Sign-On

The solution provides Single-Sign-On (SSO) features to connect to a different category of systems and devices without entering the login credentials. These are ready built-in connectors for all standard industry systems. Also connectors can be built for legacy applications/systems.

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.

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.

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

It's a challenge for an 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.

Features of

Compliance

Customized Reporting

The regulatory standards mandate the IT risk management team to provide detailed information about access control policies needed for safeguarding ritical 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 | PAM'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 everycommand/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.

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.

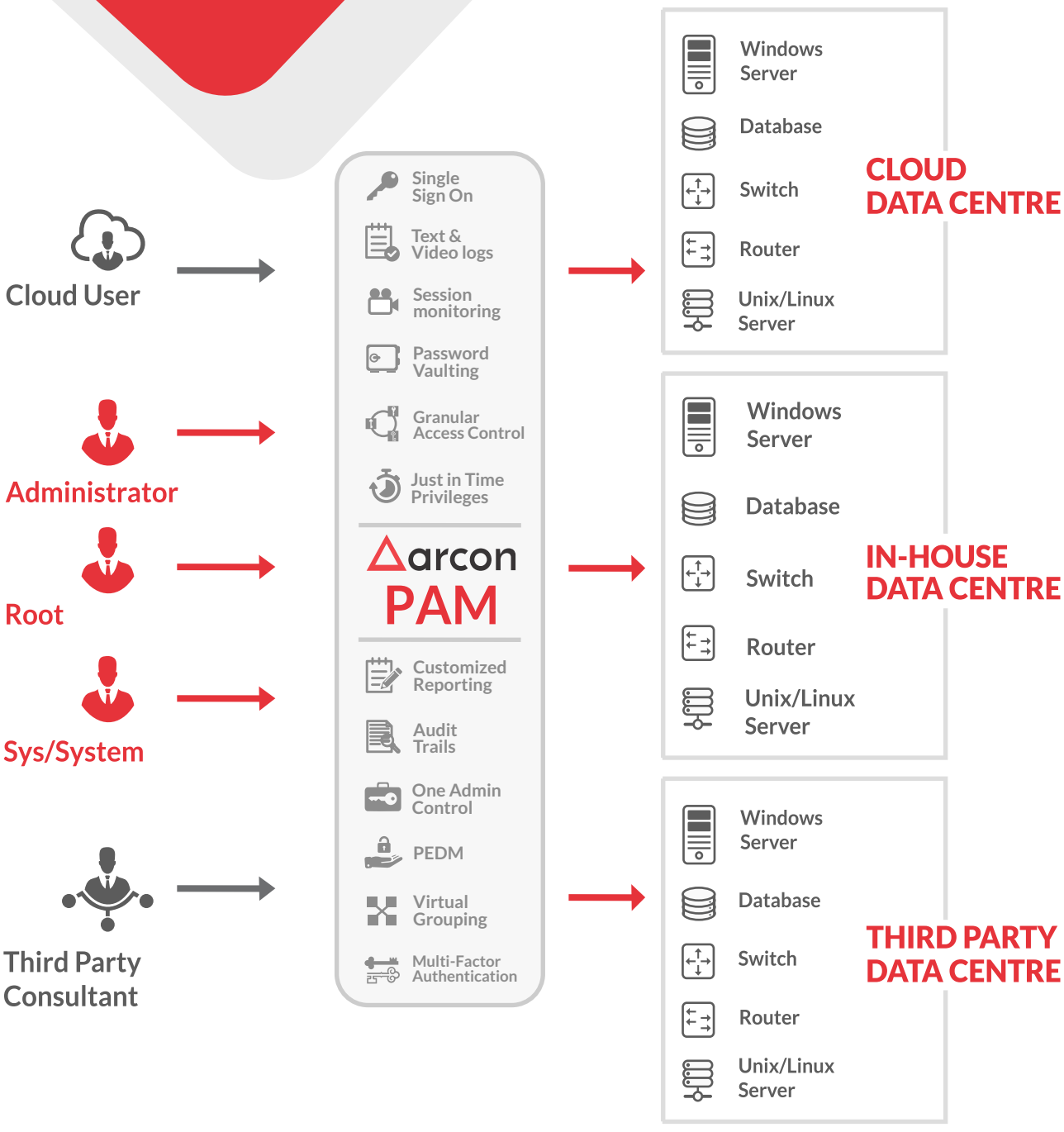
arcon

ARCON | PAM

Benefits

- Helps to meet compliance with global Information Security standards such as SWIFT CSCF, PCI-DSS, HIPAA, SOX, NESA (UAE), the EU GDPR among many other regulations
- Ensures privileged access to target systems only on a 'need-to-know' and 'need-to-do' basis
- Implements the principle of least privilege to restrict access to critical systems and minimize the threat surface
- Provides seamless workflow matrix to administrate day to day use cases
- Offers Just-In-Time privileges to ensure access to systems and applications according to when and how long the task is required
- Offers a proprietary unified governance framework that addresses and mitigates risks across the network
- Helps organizations to implement Zero-Trust security framework to strengthen security infrastructure
- Helps administrators with real-time threat analytics
- Identifies and detects malicious insiders with seamless monitoring of the privileged tasks and notifies the administrator about any suspicious behaviour
- Enhances overall IT efficiency and ensures security of confidential data

Product Architecture



Conclusion

ARCON | Privileged Access Management (PAM) is a comprehensive solution that manages, monitors and controls the security of an increasing number of privileged accounts in modern enterprises. Guidelines provided by EU GDPR, PCI-DSS, SWIFT, ISO-27001, BASELIII, HIPAA, SOX and other global regulatory standards have made it mandatory for organizations to incorporate necessary IT safeguards to protect privileged accounts from unauthorized activities. Fortifying privileged identities with ARCON | PAM enables firms in fulfilling regulatory requirements from a single platform.

ARCON | PAM solution provides a layer of abstraction over the underlying IT infrastructure fabric that enforces users to logon by using user-id, passwords, and a unique OTP (One Time Password). Also, this solution has the ability to provide required user access on a “need-to-do” basis and can track their activities distinctly even if they are privileged users.

The solution not only provides a security umbrella to the underlying IT infrastructure and data but also maintains a complete audit trail of activities linked to privileged accounts. This tool identifies vulnerabilities and assesses risks at various levels like operating systems, databases, servers and notifies the administrators on an immediate basis.

arcon

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management

Connect with us