KuppingerCole Report

EXECUTIVE VIEW

By Paul Fisher

November 03, 2020

ARCON PAM SaaS

Privileged Access Management (PAM) must evolve if it is to meet the demands of different types of organizations and IT architecture. A one size fits all approach does not work in a world where access to privileged accounts is changing. Organizations need PAM solutions that fulfill security requirements but also deliver convenience, rapid deployment, and cost efficiency. Therefore, PAM delivered as a service is gaining traction in the market and, in this report, we consider the merits of ARCON PAM SaaS.

By **Paul Fisher**
pf@kuppingercole.com

Content

1 Introduction

Privileged Access Management (PAM) solutions are critical cybersecurity controls that address the security risks associated with the use of privileged accounts in organizations and companies. Traditionally, privileged users were mostly confined to various levels of IT administrator but in modern organizations many more users need access to privileged accounts, and the definition of what constitutes privileged has also changed. This now includes access to sensitive data and information assets such as HR records, payroll details, DevOps services, financial information or intellectual property, and even social media accounts.

In recent years, PAM solutions have become more sophisticated making them robust security management tools in themselves. While credential vaulting, password rotation, controlled elevation and delegation of privileges, session establishment and activity monitoring are now almost standard features, more advanced capabilities such as privileged user analytics, risk-based session monitoring, advanced threat protection, and the ability to embrace PAM scenarios in an enterprise governance program are becoming the new standard to protect against today's threats

Among the key challenges that drive the need for privilege management are:

- Abuse of shared credentials
- Abuse of elevated privileges by unauthorized users
- Hijacking of privileged credentials by cyber-criminals
- Abuse of privileges on third-party systems
- Accidental misuse of elevated privileges by users
- The requirement to perform attestations on privileged users and admin accounts
- Discovery of shared accounts, software, and service accounts across the IT infrastructure
- Identifying and tracking of ownership of privileged accounts throughout their lifecycle
- Auditing, recording, and monitoring of privileged activities for regulatory compliance

So, while demands on PAM have increased, the type and size of organizations needing protection for privileged accounts is also changing rapidly. Smaller and specialist businesses realise that the number of privileged accounts is increasing as they adopt a more digital business model, or they are part of a supply chain that requires third party access to their own files and services. The pattern of increased home working due to Covid 19 in 2020/21 has created demand for privileged access from remote endpoints, which may not be secure as they should be.

PAM vendors are responding to all these changes in different ways, by adding more specialised modules to

already comprehensive platforms while other, often newer, vendors are targeting one aspect of the PAM market demands such as securing DevOps. But as PAM requirements become more complex for organizations to manage on their own, vendors are also starting to deliver PAM as a service in which management, security and maintenance of privileged accounts can be undertaken by the vendor, usually as cloud based service or purchased from a third party MSP. While not exclusively, this solution often appeals to smaller businesses or larger enterprises seeking to run a hybrid PAM set-up with the SaaS solution used in specific LOBs. In this Executive View we look at ARCON PAM SaaS and how its fits into this growing market.

2 Product Description

Founded in Mumbai 2006, ARCON has established itself as one of the leaders in Privileged Access Management (PAM) and is now entering the SaaS market with ARCON PAM SaaS. ARCON has local presence in UK, Canada, South Africa, Dubai, Malaysia, Philippines and Kenya with its operations and R&D center in Mumbai, India.

ARCON PAM SaaS is based on implementing a zero-trust security framework for privileged accounts and does not lack for any features that are provided in the regular on-premises suite that ARCON also provides. The company proposes four typical customer models for the product: Small and Medium (SME), Enterprise, Managed Service Provider (MSP) and the Partner SaaS model.

These last two sectors are important. KuppingerCole believes there will be significant growth in the number of third-party providers of PAM services in the next five years. While the models are different, the core product is the same giving all customers the option to pick and choose features and capabilities as they need and not worry about updates as these are automatically applied by ARCON.

There will also be significant growth in smaller businesses looking to use an established PAM vendor provider like ARCON to provide PAM as a Service directly. In this instance, ARCON's customers can self-register for the service directly from the ARCON website and take it from there. All connections to Target Devices are via Secure Tunnel (SGW) or via Application Streaming (HTTPS with TLS 1.2) with Session Isolation using the Application Gateway (AGW) Component of the full ARCON PAM Solution.

In the Enterprise Customer Model ARCON suggests that large companies can connect data centres from locations across the world into a single instance of ARCON PAM and be managed from one central console. Alternatively, customers can separate PAM operations into regions for compliance reasons, for example, and still benefit from all the hosting benefits. The MSP model provides the same functionality but delivers flexibility to the MSP provider to deliver PAM services to clients in the cloud or on premises and the MSP can manage multiple customers from a single installation of ARCON PAM. To meet compliance demands, multiple partitioning techniques are used to separate client data.

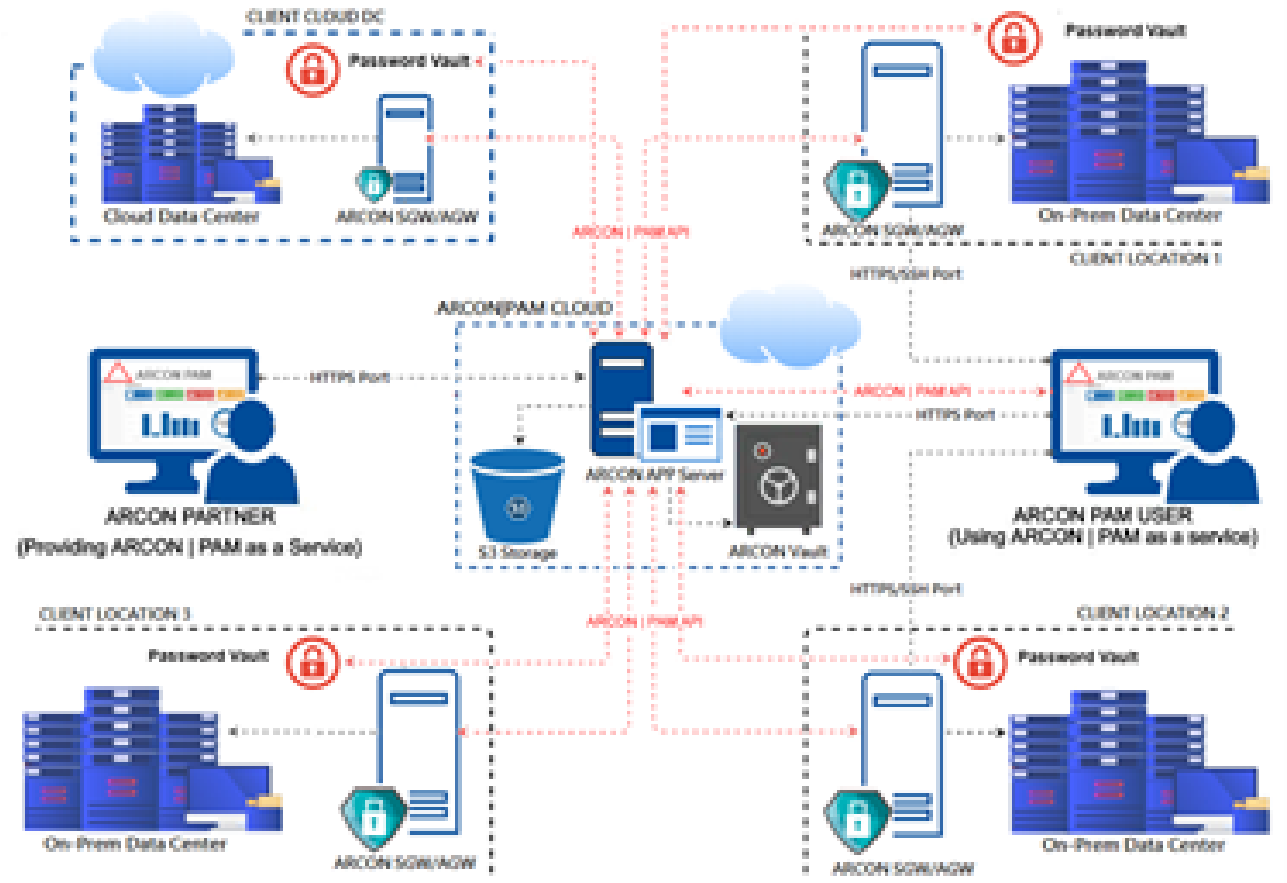

Figure 1: Schematic of how ARCON Partner SaaS model allows organizations to manage privileged accounts in vendors or other third parties. (Source: ARCON)

Finally the Partner SaaS model allows larger companies to host PAM services for vendors or other third parties which provides a useful option for modern complex supply chains and gives organizations peace of mind that partners are protecting privileged accounts to the same standard. All cloud-based solutions are designed to run under AWS.

ARCON PAM SaaS in use

ARCON has based all set up and configuration around a dedicated cloud portal that allows customers or partners to create the set up best suited to their own organization or for their clients. The pages within this are clear and easy to understand (full of pop down menus) which reduces set up time to the minimum. The Admin Registration Form (see Figure 2) is a good example which makes signing up to the service quite a consumer like experience. After that, a series of online prompts will take the user through furthers steps that allow companies to be registered with the service and further divided into Line Of Business (LOBs) if so required. Customers can also set responsibilities for admins within the organization through the same portal.

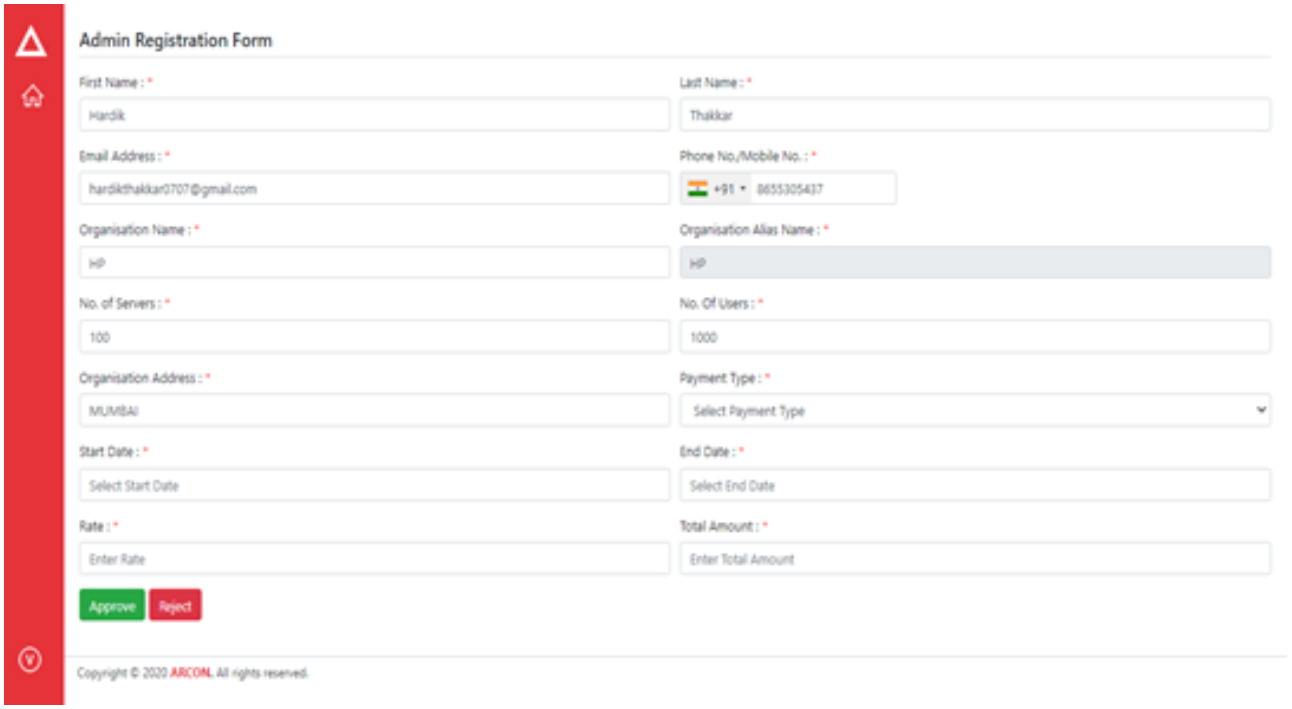

Figure 2: The sign-up form for administrators to register for ARCON PAM SaaS with drop down menus and payment type options (Source: ARCON).

Those customers running ARCON PAM SaaS as an MSP or on behalf of vendors also benefit. Here they can access data such as number of companies, LOBs and users being hosted as well as the number of services available. Other features include Direct login, multiple sessions in the same window, switching between sessions and custom folder creation.

Buyers of ARCON's PAM SaaS still benefit from ARCON's existing product architecture with built-in high availability, real-time password replication and automated recovery features. These enterprise grade features enable the platform to support multi-cloud, multi-tenancy and third-party remote access use-cases which are now common features of digital organizations. Security and convenience are enhanced by OTP authentication for privileged session initiation and integration with third party biometrics providers. ARCON also supports integration with hardware-based OTP tokens from Entrust and RSA SecurID.

ARCON's tools for privileged user account discovery are also notable for their flexibility. These can be run on-demand & detect all accounts across designated servers and/or endpoints and correlated with existing on-boarded privileged accounts. Once discovery has been completed admins can analyse accounts and refine into Local/Domain or Privileged/Non-Privileged, for example. Privilege IDs can be onboarded in bulk by using a bulk import feature embedded within the solution.

Any leading PAM solution in today's market should provide a substantial range of connectors and ARCON PAM SaaS boasts more than 300 integrations which are available through a GUI making it easier for partners and clients to integrate applications and services.

Smart session monitoring analyses video, images keystrokes and face recognition to detect suspicious

activity and provides comparison of live metadate with recorded activity. To further prevent fraudulent access at source, ARCON PAM SaaS features Just-in Time provisioning that provides limited time access, ephemeral accounts and on-demand privilege elevation that also time out. Modern organizations increasingly need greater access flexibility for privilege accounts users such as DevOps and multi-cloud users. Out of sync credentials can be auto healed and integrated within analytics and SIEM solutions. Password rotation tools are a strength and MSPs will benefit from the wide support for many standard enterprise applications such as Windows, SAP, Oracle, Cisco, Juniper, VMware and many others.

3 Strengths and Challenges

With IT environments becoming more complex and the increase in privileged accounts putting extra pressure on managing these environments, a feature rich PAM platform delivered as a service makes good sense. The strength of ARCON's PAM SaaS is that it is equipped with the technology and features that made ARCON one of the Leaders for Innovation in the KuppingerCole PAM Leadership Compass 2020

ARCON has understood the market well by modelling its SaaS platform for Small and Medium (SME), Enterprise, Managed Service Provider (MSP) and Partner SaaS models. Of course, PAM as a Service in the market is not unique but ARCON has made good strides in its understanding of ease of deployment, usability and how different environments may want to deploy PAM as a service to their own needs. Interoperability and scalability have seen a further boost with ARCON now supporting 300 integrations which are available through a GUI making it easier for partners and clients to integrate applications and services.

ARCON has a conventional vault at the centre of password management and many on-premises iterations would be glad of the reassurance that often comes with a well-protected vault, and ARCON provides that. However, while ARCON PAM SaaS does support JIT and OTP and other ephemeral access protocols we would like to see in addition an option for password less and vault less PAM in future revisions. The demands of DevOps and other agile teams and the risks of storing passwords in the cloud are such that we feel the market is moving towards providing these types of solutions, particularly in hybrid PAM environments.

Overall, ARCON PAM SaaS solution, offering capabilities across different IT architectures, is a recommended product for managing privileged access in a heterogenous IT environment and one that deserves further technical evaluation.

Strengths

- Takes away deployment, maintenance and provides lower operating costs
- Simple configuration and admin tools
- Highly scalable and flexible enough to meet different customer models
- Helps shift focus from infrastructure maintenance to security enhancements
- Large number of connectors improves interoperability and legacy fit
- Well suited for SMBs and mid-market organization

Challenges

- We would like to see adoption of vault free and password less options for hybrid and multi-cloud environments
- Increasing but limited penetration in North America and European markets but this should improve
- Limited to AWS

4 Related Research

Advisory Note: Trends in Privileged Access Management for the Digital Enterprise – 71273
Architecture Blueprint: Access Governance and Privilege Management – 79045
Blog: PAM Can Reduce Risk of Compliance Failure but is Part of a Bigger Picture
Blog: Privileged Access Management Can Take on AI-Powered Malware to Protect
Blog: Taking One Step Back: The Road to Real IDaaS and What IAM is Really About
Leadership Brief: The Information Protection Life Cycle and Framework: Acquire and Access – 80371
Leadership Brief: The Information Protection Life Cycle and Framework: Control Access -- 80372
Leadership Brief: Privileged Access Management Considerations – 72016
Leadership Brief: Identity Fabrics – Connecting Anyone to Every Service – 80204
Leadership Brief: Leveraging Identity Fabrics on Your Way Towards Cloud Based IAM -- 80501
Leadership Compass: Identity Provisioning – 70949
Leadership Compass: Identity Governance & Administration – 71135
Leadership Compass: Privilege Management – 80088

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded back in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.