KuppingerCole Report

EXECUTIVE VIEW

By Paul Fisher

October 19, 2021

Saviynt Cloud PAM

Saviynt Cloud PAM is a privileged access management solution engineered to work primarily as a service and sits as part of the Saviynt Enterprise Identity Cloud platform. It is a modern and competitive PAM package that performs most of the essential components of a PAM solution with a zero-footprint deployment model. It should be of interest to a wide number of organizations.

By **Paul Fisher**

pf@kuppingercole.com

Content

1 Introduction 3

2 Product Description 5

3 Strengths and Challenges 8

4 Related Research 10

Content of Figures 11

Copyright 12

1 Introduction

PAM platforms are critical access and security controls that address the risks associated with the use of privileged access in organizations and companies. It is recognized that most successful cyber-attacks involve the misuse of privileged accounts. And misuse is enabled by poor management of privileged access using old or inadequate PAM software (or even none!), out of date policies and rusty security processes. The recent rise in ransomware has given organizations another reason to consider PAM as many of these attacks target privileged accounts as a gateway into wider enterprise networks.

The dangerous activities that PAM must control include abuse of shared credentials, misuse of elevated privileges by unauthorized users, theft of privileged credentials by cyber-criminals and abuse of privileges on third-party systems.

While PAM platforms have been around for around 20 years, the demands of digital transformation and wholesale structural changes to IT architecture have intensified interest in Privileged Access Management software and applications -- across all market sectors. While many assets remain on-premises or in private data centres, many organizations are also using the cloud for infrastructure, storage and SaaS applications. PAM must keep up with these developments.

KuppingerCole research shows that the PAM market is responding and growing because of these challenges and is in a vigorous period of growth and innovation. Part of this is flexibility in purchasing options with growth in subscription models and SaaS options, although licensing and maintenance deals still dominate the sector. KuppingerCole believes that as PAM moves to a dynamic operating model to deal with dynamic IT architectures, SaaS and flexible purchasing options will become more popular with customers not wishing to be tied into technology that does not evolve fast enough for their changing demands.

A typical IT estate will include applications, on-premises architecture, data centres, Microservices, orchestration platforms and multi-cloud infrastructures. Somehow, organizations need to manage PAM all through this new digital landscape. KuppingerCole considers there will be demand among organizations of all sizes to outsource some or all of the deployment and operation of PAM to Managed Service Providers (MSP). In addition, more PAM vendors will offer full PAMaaS run from the cloud on behalf of their clients - this will require new commitments of trust between client and provider, not least in protecting data privacy and honouring Service Level Agreements (SLA).

Legacy PAM solutions scan IT environments at regular intervals, but progressively these intervals can't keep pace with the rate at which, for example, cloud resources and microservices auto-scale, leaving them periodically at risk. Managing the security of PAM consistently and uniformly applying governance is now much more complicated.

All of which means that many businesses will be less inclined to manage PAM themselves and drawn to the ease of use, deployment and auto updates that PAMaaS offers. This trend will not be restricted to smaller

businesses, or those without large in-house technical teams -- although this is an obvious target market - but also to larger corporations that possess hugely complex IT estates where PAM plays a critical role in protecting specific high-value operations.

While many public clouds come with some form of PAM application and security commitments in SLAs, these differ across proprietary Cloud Service Providers (CSP) making it hard to maintain consistent security access management in multi-cloud, multi-provider environments. What is desirable is a dedicated PAM solution that handles all modes of identity across multiple clouds and hybrid IT infrastructures. The good news is that organizations have never had more choice in PAM tools and deployment options to match their IT environments, processes, and supply chains. In this Executive View we consider the PAMaaS option vended to the market by Saviynt.

2 Product Description

Saviynt is a US based company founded in 2009 that specializes in Identity and Access Governance. It has taken its learnings in Identity Management to integrate fully-featured PAM to the Saviynt Enterprise Identity Cloud platform which can also administer Access Governance, IGA and PAM from a common interface to all enterprises. In addition, Saviynt Enterprise Identity Cloud platform also includes Application Access Governance, Third-party Access Governance and Data Access Governance. Buyers can choose any combination of services in the knowledge that they are scalable and natively compatible, easing the process to add IAM capabilities across an organization.

Saviynt Cloud PAM runs as a service on the three leading public cloud platforms: GCP, AWS and Azure. Saviynt designed the solution to be fully cloud native and to utilize APIs to integrate with as many leading enterprise applications as possible. These include enterprise stalwarts such as Office 365, Salesforce and Workday.

Figure 1: Savinyt Cloud PAM sits within the Saviynt Enterprise Identity Cloud (Source: Saviynt).

Saviynt Cloud PAM is a lean code platform that results in zero on-premises footprint which should accelerate deployment and automate maintenance and upgrades applied by Saviynt. There are also advantages from this architecture to enhance High Availability and Just in Time (JIT) privileged access - two of the more important capabilities for modern cloud and DevOps environments. The tool is designed to allow

enforcement of least privilege access policies by hiding credentials from end users and automatically rotating credentials in a vault. If required, the solution comes with a vault included OOTB based on HashiCorp but is transparent in use to customers. While Saviynt Cloud PAM resides in the cloud, customers can control usage and management from consoles that sit on-premises, cloud or in hybrid stacks. In a deployment on Google Cloud Platform a major customer was able to import and correlate 96k accounts and around 700k entitlements from its own console; administrators therefore have a good range of control over this PAMaaS package from the well-designed dashboards.

For a platform designed to manage multi-cloud and hybrid-cloud environments its sensible that Saviynt has built-in Cloud Entitlements Manager (CIEM) features - which is hugely beneficial for keeping a record of complex cloud usage (scaled up and down) and for agile and fast-moving DevOps environments. In addition, as part of its converged Enterprise Identity Cloud (EIC) platform, Saviynt's cloud PAM has access to fully compatible IGA features, a speciality of Saviynt.

Within the product itself are account discovery, session recording and session management as well as more advanced features such as Risk Analytics, credential-less access and a risk and controls library. The guiding principles behind the platform are reducing numbers of static privilege accounts in an organization and avoiding storing unused credentials in a vault. This makes it potentially a good choice for those organizations looking to enable Zero Trust policies and Zero Standing Privilege environments in their cloud and on-premises environments.

Saviynt Cloud PAM does not use jump boxes for access which should make deployment faster, reducing time to value for buyers. The web-based interface is designed to be user-centric and in this the company has succeeded in creating a very clean and simple interface, in line with current practice.

Most recently Saviynt has added some significant new capabilities to the platform. These include continuous discovery of cloud workloads and entitlements plus always-on monitoring of services and workloads for security errors or misconfigurations. A new Risk Exchange tool allows bi-directional data integration with leading 3rd party solutions from SIEM and Vulnerability Management vendors. There is now also Automated Backdoor Entry Protection, which can identify backdoor accounts and automatically disable or delete vault access based on policies. An "alert and mitigate" function adds to the governance and security capability of Saviynt Cloud PAM. In addition, are the features to manage privilege access for both infrastructure and apps and "PAM for Any App" - the ability to manage any app directly through Saviynt Cloud PAM.

For the near future, Saviynt is addressing the increased importance of DevOps, CI/CD and Infrastructure as Code (IaC) teams within organizations. Its pipeline includes plans to change the way DevOps code deployment entitlements are managed by switching the focus from managing access in the OS (via SSH/RDP) to managing commands in orchestration software such as Terraform (or similar), with changes deployed in updated container images. Saviynt PAM would then regulate CSP (cloud security provider) roles needed by pipelines executing such code, managing real time permissions for these pipelines and providing a risk-based audit view of actions.

It was a bold move to create a PAM solution that is primarily as a service from the cloud (it can run on premises and in hardware if desired) but it looks increasingly like a sensible decision. It gives Saviynt control over iterative development, upgrades and maintenance for customers, improving their security posture.

Saviynt PAM Cloud is a welcome addition to the ranks of PAM software, taking PAMaaS solutions into the mainstream as well as reducing reliance on passwords for end users. It goes some way to closing the gap between security and convenience. The vendor also has ambitious plans to develop capabilities further, especially in the realm of CI/CD and DevOps production environments. For any organization looking to manage and scale privileged access in complex and demanding IT environments we would highly recommend further investigation of this software package.

3 Strengths and Challenges

Building on their experience gained in IAM and IGA solutions, Saviynt has produced a competitive PAM package that benefits fully from its cloud native architecture. There are undoubted deployment and operational benefits from PAM software that sits in the cloud and runs as a service. Although the software can be installed on-premises, it clearly has been designed for a future where cloud applications and services are dominant and organizations grapple with ever more complex IT architectures.

It also goes some way to reducing reliance on passwords by enabling password-free login for privileged users, although we would like to see Saviynt take the next bold step and remove passwords and vaults altogether. That the company has not developed a vault of its own suggests that its hunch is to remove reliance on passwords soon. In addition, plans to run permissions natively within containers and orchestration platforms for DevOps are exciting and we hope to see this, or a version of this, become the default for all privileged access across in a product development. We believe Saviynt is ahead of the curve in understanding PAM's role in Cloud Infrastructure Entitlement Management (CIEM).

Some organizations may still prefer more traditional PAM platforms that run on-premises and are completely managed by the customer. Vendors of these platforms are also developing PAMaaS to compete with Saviynt and so the challenge for the company is up its marketing and messaging that its cloud native, lean code platform delivers deployment and operational benefits and is particularly suitable for multi-cloud environments. It also has an added advantage of native integration with the IGA and Identity Management tools found in Saviynt Enterprise Identity Cloud platform.

Strengths

- Integration of functions designed in from the start, takes PAMaaS to a new level
- Saviynt has clearly thought about how cloud apps and infrastructure affect PAM and worked to accommodate that
- The company has exciting plans to embed PAM within the code and infrastructure layers dispensing with permissions at the application/OS layer
- A good step towards reducing reliance on passwords
- Good control of redundant IDs and unused passwords

Challenges

- Saviynt may wish to explore a completely password free platform in the future
- This is a solid and innovative platform that now needs effective marketing to increase its customer base
- This is a fresh approach to PAM but still lacks some traditional PAM capabilities – but this may not matter for some deployments
- Next step would be to integrate native DevOps tools and improve Machine Identity capability – this is registered in the pipeline.

4 Related Research

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: Privileged Account Management Considerations - 72016
Leadership Compass: Identity Provisioning - 70949
Leadership Compass: Identity Governance & Administration - 71135
Leadership Compass: Privilege Management - 72330

Content of Figures

Figure 1: Savinyt Cloud PAM sits within the Saviynt Enterprise Identity Cloud (Source: Saviynt).

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 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.