KuppingerCole Report

EXECUTIVE VIEW

By Paul Fisher

September 17, 2020

Fudo PAM by Fudo Security

Fudo Security's PAM solution is the company's primary product in the expanding PAM market. In the last few years PAM has evolved into a set of targeted technologies that addresses some of the most urgent areas of business security in a period of rapid technological change. Digital transformation, Cloud, and Hybrid IT environments are creating new demands and innovative PAM solutions are emerging to meet these challenges.

By **Paul Fisher**

pf@kuppingercole.com

Content

1 Introduction

Digital transformation is no longer optional for businesses and organizations if they wish to stay competitive and deliver greater value to customers. But as they seek to embrace the advantages of Cloud, IoT, AI and Big Data projects across extended infrastructures, organizations need to be aware of the cyber security, compliance, and identity risks that digital transformation also creates.

While these risks are serious, they can be significantly reduced through intelligent, fit for purpose and structured deployment of security solutions. As agile access and identity requests are a prime characteristic of a successful digital environment it follows that one of the most important tools to manage this securely is Privileged Access Management (PAM).

Privileged Access Management (PAM) solutions are critical cybersecurity controls that address the security risks associated with the use of privileged access in organizations and companies. Traditionally, there are primarily two types of privileged users:

Privileged IT Users – those who need access to the IT infrastructure supporting the business. Such permissions are usually granted to IT admins who need access to system accounts, software accounts or operational accounts.

Privileged Business Users - those who need access to sensitive data and information assets such as HR records, payroll details, financial information or intellectual property, and social media accounts.

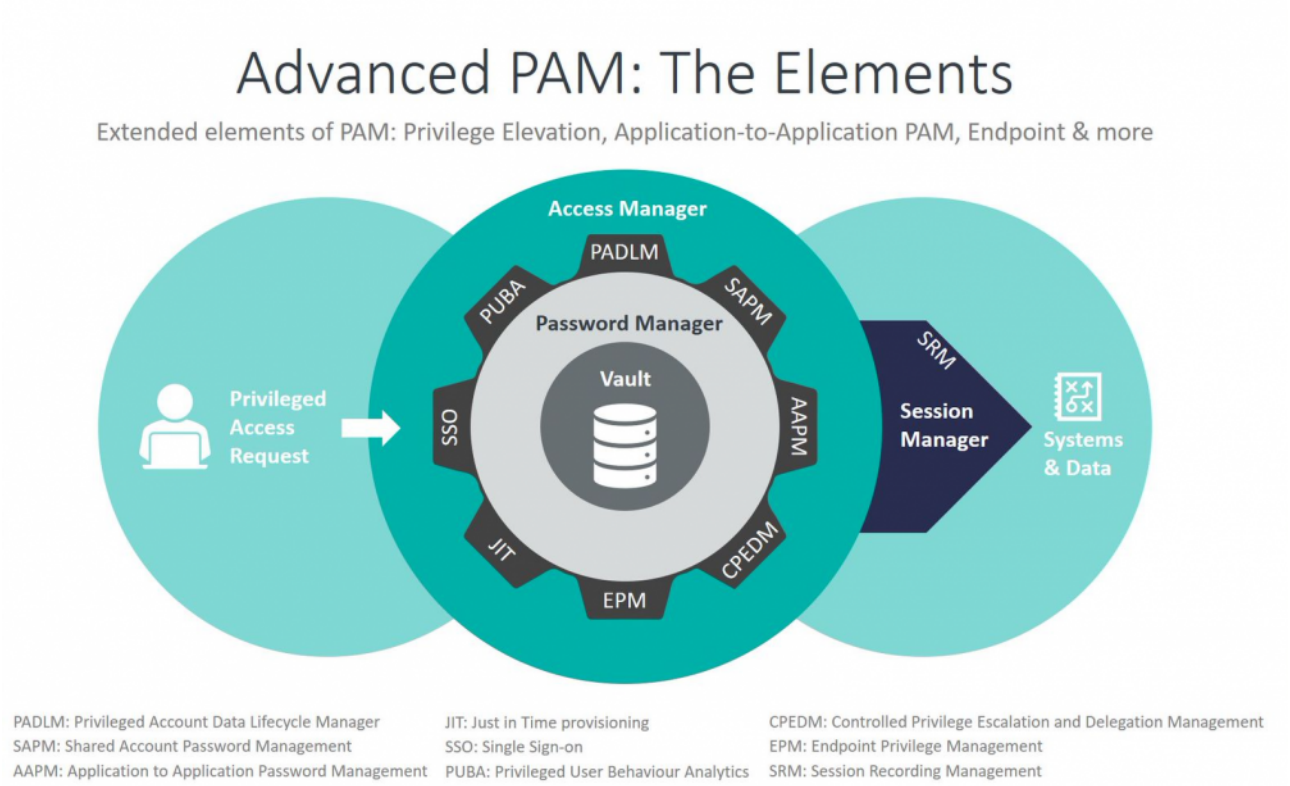

Figure 1: Advanced PAM features. As the market demands have developed vendors have added more functionality to their solutions.

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 user
- The requirement to perform attestations on privileged users and admin accounts
- Vulnerability of endpoints that provide access to privileged accounts

Furthermore, there are several other operational, governance and regulatory requirements associated with privileged access:

- Discovery of shared accounts, software, and service accounts across the IT infrastructure
- Identifying and tracking of ownership of privileged accounts throughout their lifecycle
- Establishing Single Sign-on sessions to target systems for better operational efficiency of administrators

- Auditing, recording, and monitoring of privileged activities for regulatory compliance
- Managing, restricting, and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems
- Managing, restricting, and monitoring administrative access of internal users to cloud services

In addition, organizations are now faced with tighter budget controls after the Covid-19 crisis which also highlighted the need for secure access to SaaS applications and databases from home offices or other remote locations. They need to balance cost, time to value and security for any new IT investment.

Users also need fast and easy access to applications, files, databases, and servers which calls for greater attention paid to the design of the security and productivity balance within PAM tools. In recent years, PAM solutions have become more sophisticated making them robust security management tools. While credential vaulting, password rotation, privilege delegation and activity monitoring are now more common, more advanced capabilities such as privileged user analytics, risk-based session monitoring, advanced threat protection, and the ability to embrace PAM into an enterprise governance program are the new standard to protect against today's threats in complex environments.

2 Product Description

Fudo Security is a relatively new player in the PAM market having launched its platform only in 2016, but the company shows technical ambition and is committed to rapid product development. As befitting a relatively young software product, it has a modern and crisp interface that allows a good degree of UX customization with drag and drop and resizable tiles or “dashlets” as the vendor describes them - a little like Windows 10. The same customization tools can be used for presentation of data – which is useful for analytics, reporting and behaviour pattern management.

Fudo Security takes a slightly different approach to PAM which offer some innovative and advanced ideas. Fudo Security believes that session management and recording are the most important parts of privileged access, thus the platform focuses on the component’s password manager and session manager as well as account discovery and endpoint protection. That does not mean it is not a competent product, however, or that users would miss out on robust PAM security with Fudo. The session manager is well featured; it fully supports HTTPS recording of users’ interaction with web services as well as support for 12 protocols including RDP, VNC, SSH and Telnet. Of note is the innovative use of raw data capture which is faster and easier to analyse then the more conventional use of screen capture tools.

Password management is operated through pre-defined scripts and in-house plug-ins that can be used to automate the process. Admins can write their own scripts as well for any account on any device offering more customisation and flexibility. There is almost limitless storage of archived sessions available if customers choose - the Fudo appliance can be connected to a large Fibre Channel (FC) array or use a thin volume, offering up to 500 TB of searchable and shareable session storage.

The platform supports full bit-by-bit protocol recording of sessions without using screenshots or partial records such as Window names only. Optical character recognition (OCR) is supported in graphical sessions which enables text search on any screen (including Cyrillic support) and works with most graphical protocols, including RDP, VNC and recorded web sessions – a strong point. Another useful feature is the ability to calculate session activity (in real-time) and create reports based on user activity which has the business advantage of checking time-based invoices from consultants or other contractors using privileged accounts. The password and session recording tools of Fudo are up there with some of the best in class and given the ever increasing number of users looking to access privileged accounts the company is right to focus initially on this aspect of PAM and apply modern software design.

However, there is more to the product; some strong technical innovations are worth mentioning and that bode well for the future. Fudo Security PAM is an 100% agentless solution so no software needs to be installed on servers or clients which may well contribute to Fudo Security’s less than a day deployment measurement. Actual times will vary depending on circumstances, but the lean nature of the solution should make deployment considerably more rapid than many competing products for a good number of customers, and the one-day timescale easily in sight. In fact, one of Fudo’s biggest customers in the energy sector, Gas Storage Poland confirmed that it achieved this target.

Multi-factor Authentication (MFA) is highly important for PAM these days and here Fudo delivers with

support for OATH (Google Authenticator) authentication currently, as well as SMS and Duo authentication support also included. There is no need to change authentication configurations on the server side. Fudo also offers Gateway mode support, which allows security managers to implement a transparent solution for administrators. This transparency allows admins to see how users are trying to connect to privileged accounts and force them to use PAM if necessary. This is useful if they are connecting via an untrusted VPN for example, stopping users slipping under the radar. That said, the UX for end users hides all such complexity and the User Access Gateway portal provides easy access to servers – the user is presented with a list of servers in one place, and a privileged session start can be initiated by pressing the “play” button - a thoughtful touch and one that adds greater efficiency to PAM in digital environments. Convenience and security at play.

Like others in the market, Fudo has added AI functionality in the latest version of its solution which allows session analysis in real time. However, Fudo Security has gone further than rivals with AI used to detect biometric anomalies such as unusual mouse or typing movements within the CLI or dashboard components. This should detect rogue users and abuse of admin or end user accounts if human computer interaction suddenly differs from the norm.

There is true active-active cluster solution – all the cluster nodes are used to provide session connectivity instead of active-passive mode operation and the number of cluster nodes is unlimited, according to the company. Shared session support is strong as the solution can show who did what in any given session – the original user or any person that joined the session, i.e. an operator or an administrator. Again, this helps with governance and faster analysis of events.

There is double encryption across the platform besides the encrypted file system layer, all sensitive database fields are encrypted using a Master Key, unique to Fudo PAM. There is also integration with third-party password vaults including CyberArk, Lieberman and Thycotic thus providing flexibility for mixed or hybrid PAM deployments.

The platform can entirely separate the end user from the internal networks by the use of a “golden image” Chromium-based browser that streams the content directly to the users – a kind of proxy host for files being accessed elsewhere. This is a good GRC focused move and one that works well. The latest release also allows users to run web applications such as a VMWare console or secure access to social media accounts including Twitter, Facebook and LinkedIn.

3 Strengths and Challenges

As befits a young and well-architected PAM platform, Fudo PAM has a modern and crisp interface which allows a great degree of customization with the drag and drop and resizable tiles available. Providing a positive user experience is highly important but often overlooked by many IT vendors so it is good to see Fudo Security make the effort here. The same customization can be used for data presentation which makes it useful for simplifying reporting and pattern management.

The company believes that session management is the most important part of PAM and this view is likely to be shared by many potential buyers who are looking to manage growing numbers of privileged accounts in their environments. Therefore, the company has sensibly focused on getting the fundamentals of PAM right while adding in some innovative features to those, such as the use of AI to detect anomalous physical behaviour at endpoints and full data capture in SRM mode.

We like that the session manager also supports full HTTPS recording of user's interaction with web services. Password management is also a strong point here. Changes to passwords can be made through pre-defined scripts while in-house plug-ins automate password management. External user passwords can be created by hand or can use the standard LDAP password. While the world remains wedded to passwords (for good or bad) for many access situations, it is good to see a vendor making password management as seamless as possible.

Fudo Security PAM supports SIEM tools including ArcSight and Splunk but there are still features missing from this solution in terms of PUBA and PADLM, for example. However, as most customers look for SAPM and Session Management capability only this is not a handicap in a solution that has been designed from the ground up – Fudo can easily add functionality as required in keeping with the lean nature of the software design. Add in the well-designed interface and unique machine learning tools that can detect unusual behaviour and it will be of interest to a good number of organizations. The one-day deployment time seems possible due to a compact self-contained appliance footprint, and at least one customer has achieved this.

Finally, Application-to-Application Password Management (AAPM) is now fully supported with a one-time-password tool for a M2M access, which includes DB sessions (MySQL and MS SQL) as well. We look forward to further development of this well-conceived and executed PAM solution that should appeal to many buyers in the PAM marketplace.

Strengths

- Crisp design, drag and drop customizable interface is refreshing
- Strong SRM and PSM functions with full data capture
- May appeal to many organizations looking for compact solution that does the basics well or as part of hybrid PAM environment
- Appliance and agent less based delivery offers much faster deployment and configuration than many PAM solutions
- Feels modern and should lend itself well to future development

Challenges

- A little feature light still, but will get more critical capabilities to gain traction in wider market
- Current lack of support for cloud platforms and DevOps
- Opportunity to further build partnerships with 3rd party security tools

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.