kuppingercole ANALYSTS

Devolutions Server and Remote Desktop Manager

Paul Fisher

April 24, 2023

EXECUTIVE VIEW

CISOs must provide secure, rapid access to on-premises, IaaS and SaaS computing environments. It requires a rethink on traditional approaches to authentication, including to privileged resources. This report looks at the PAM challenges companies face with many thousands of active machine and human identities now seeking access to cloud based resources. There is also a concise analysis of the Devolutions Server and Remote Desktop Manager PAM platforms.

Content

Figures

Introduction

Many successful cyberattacks involve the misuse of privileged accounts, enabled by inadequate Privileged Access Management (PAM) software, policies, or processes. Malicious activities that must be detected and controlled include abuse of shared privileged credentials, misuse of elevated privileges by unauthorized identities, the theft of privileged credentials by cybercriminals, and abuse of privileges on third-party systems accessed via the cloud. PAM is a critical part of the Identity & Access Management (IAM) lifecycle.

Privileged status has traditionally been given to a small set of administrators who needed access to perform maintenance and upgrade tasks, mostly on networks on-premises or local area networks (LAN). In some cases, senior employees may have also been given elevated access rights for specific tasks. It is fair to say that this is no longer the case. Privilege management use cases now extend across entire organizations, with users and machine identities requiring task-based access to data, services, and applications on legacy systems but also fast growing, multi-cloud-based infrastructures.

PAM has evolved into a wider cyber security and identity management discipline as digitalization has increased the attack surface to include cloud, multiple endpoints, home working, and no secure perimeters. It brings significant benefits to every major digital business initiative, including securing applications and data in the cloud, privileged user behaviour analytics to detect anomalous privileged behaviour and supporting endpoint threat protection.

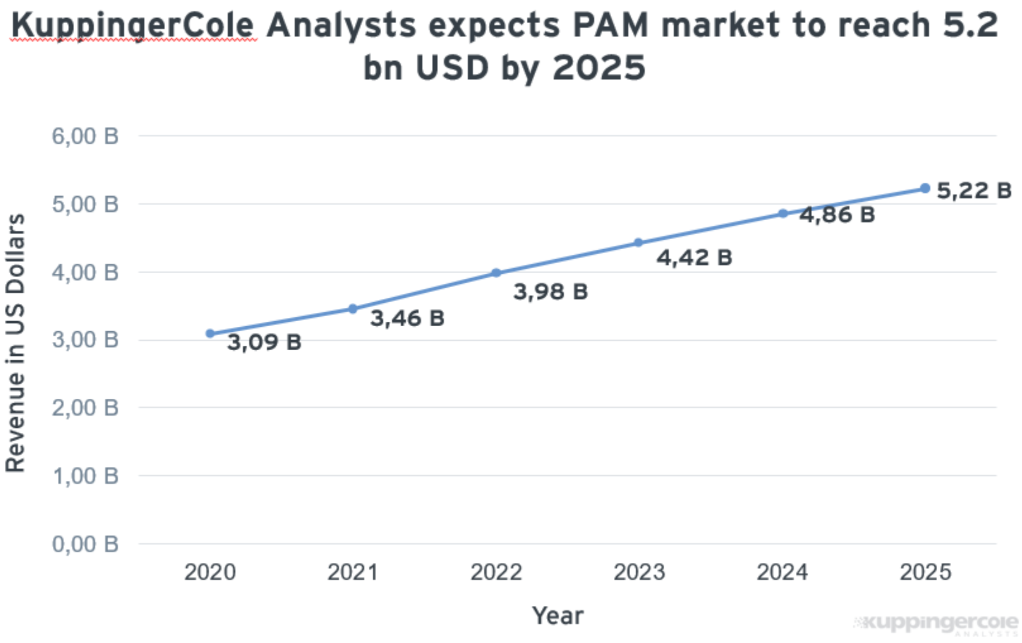

Figure 1: KuppingerCole expects to see further growth in the PAM market as software emerges to serve different types of business.

More recently, several PAM vendors have started to accommodate capabilities that support Cloud Infrastructure Entitlement Management (CIEM) for cloud-based resources, and critical cloud-based workflows such as DevOps and CI/CD projects. While there is overlap here, the demand for traditional PAM capabilities (password vaulting, credential management, full analytics, admin access, etc.) remains robust and vendor efforts to improve on those capabilities continue to drive competition.

Support for the demands of digital organizations is becoming a competitive differentiator in the PAM market. Interest in Least Privilege and Zero Trust informed architectures and policies has also grown as organizations look to secure multi-cloud environments. Buyers are increasingly aware that a well-configured and modern PAM platform can be an integral part of a Zero Trust architecture.

The PAM market continues to mature and grow (see Figure 1) with larger PAM vendors providing a full-service platform while newer entrants to the market are offering niche platforms for customers with more specialized PAM requirements. The trade-off is that full-service platforms are often more complicated to deploy and manage but the simpler niche products do not offer the same level of capabilities -so far. Buyers need to undertake due diligence before deciding on which platform is right for their business with one eye on future requirements. Some vendors, such as Devolutions featured here, offer a choice of modules that offer certain capabilities individually and full interoperability between modules for more comprehensive PAM feature sets.

Devolutions Server & Remote Desktop Manager

Founded in 2010, Canadian firm Devolutions started by selling its Remote Desktop Manager software, aimed at SMBs looking to manage remote connections, endpoints, and virtual machines. It has since added capabilities to this and the Devolutions Server module which is fully compatible with the Remote Desktop Manager to deliver an effective PAM platform.

The Remote Desktop Manager acts as a thick client remote manager that supports integrated VPN connection management with Microsoft, Linux, MacOS, iOS and Android OSes all supported. Proprietary Cisco, SonicWall and IPSec VPNs are also supported as standard, while a good number of add-on technologies and protocols can be integrated including Nortel, Avaya and Watchguard, Microsoft Remote Desktop protocol, Citrix, Vmware, FTP, SSH and others.

It4upportts a wide list of connections, including RDP, RemoteFX, RealVNC, TightVNC, UltraVNC, ICA, HDX, LogMeIn, TeamViewer, RGS, DameWare, Radmin, pcAnywhere, Telnet, RAW, rlogin, Xwindow, and Hyper-V. Significantly, credentials are automatically brokered to users; they never have access or knowledge of the plain text credentials.

Devolutions Server is a privileged and password management platform, accessible from Remote Desktop Manager or available as standalone product for organizations. In standalone mode it can be launched through any major web browser. However, Devolutions recommend buying both products for larger companies or for those with highly sensitive data to protect to get full PAM capabilities. Indeed to benefit from one of the key capabilities of the Devolutions platforms – hiding passwords from users – buyers must use both products in tandem.

Authentication services within Devolutions Server meet current industry norms; username/password, 0Auth2 via JSON web tokens plus support for OpenID. It also supports two factor authentication, supporting tools popular in the SMB space: Google Authenticator, Microsoft Authenticator and Authy. Multi-factor authentication also be configured via email, SMS or Devolutions own authenticator app. At KuppingerCole we would recommend 2FA or MFA as part of any PAM deployment, regardless of vendor, as it adds a hard layer to any PAM authentication process – one difficult for attackers to crack.

The Devolutions Workspace is an easy to read, and use, dashboard which enables administrators to grant, change, or restrict access for any user and adds extra usability to Devolutions Workspace and Remote Desktop Manager.

Administrators can add, modify and remove users based on changing needs and policies with relative ease. The clean design of the dashboard shows Devolutions understands the importance of a simple UX and easy to use tools for faster and better PAM management in complex IT environments including cloud infrastructures. It also benefits those customers who have fewer or less experienced admin staff.

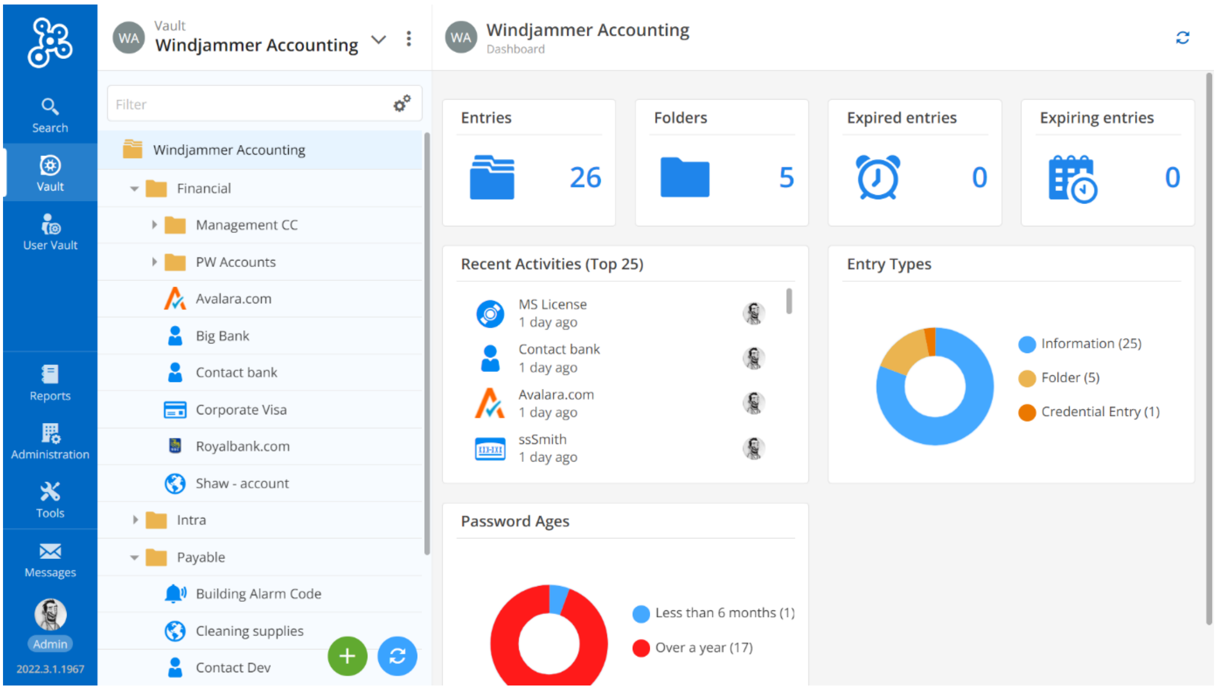

Figure 2: Devolutions Workspace delivers a neat, sensible user experience that puts admin functions and status entries within easy reach.

Devolutions Server is a full-featured shared account and password management solution with add-on privileged access components and works well with Devolutions Remote Desktop Manager. It deploys rapidly, implements well, and delivers the core features of a comprehensive PAM solution.

Devolutions Server is designed to meet the ever-expanding security requirements of SMBs, while remaining very affordable. It offers the essential PAM capabilities such as a shared password vault, which can integrate with Microsoft Active Directory and can be hosted centrally. It also offers account discovery and secure remote access.

Devolutions Gateway is another option available as an add-on to Devolutions Remote Desktop Manager to facilitate Just in Time (JIT) access to resources. It can be used with supported connection entry types (RDP, SSH, VNC, ARD, PowerShell, websites) in Remote Desktop Manager and supported data sources such as Devolutions Server and Devolutions Password Hub). Once configured to use Devolutions Gateway, new sessions will leverage JIT authorization for individual connections automatically, without additional steps. This now supports OAuth and support for Okta, better code management, support for unmanaged accounts and ticketing support via Atlassian Jira. There is now also check out approval available on the Devolutions mobile app.

Taken together, the Devolutions modules offer a compelling proposition for SMBs looking to control privileged access management if they have yet to implement a dedicated platform. But for a package that is created with SMBs in mind it has several enterprise capabilities including session recording and playback, automated password check in/check out and SSO. It lacks others, however: privileged escalation, and privileged task management for example, but does support JIT access (via Devolutions Gateway) and One Time Passwords (OTP) – good to see.

The modules are strong on account discovery focusing on identifying privileged accounts (specifically shared accounts) across various systems in a network and putting them under control. Together with the ability to remotely manage target systems running various operating systems such as MacOS, Windows, and Linux, and the password vaulting and management capabilities, this forms a PAM solution covering the essential capabilities required by SMBs, while remaining lean code base and easy-to-use features. The platform supports 2FA, AES-256 encryption, encrypted communications over HTTPS using TLS, IP restriction and time-based, Role-based (RBAC), DAC, Application-level restrictions.

Devolutions continues to innovate and add capabilities to the platform components with 0Auth support for Azure Active Directory coming. Emergency (break glass) access should ID provider software fail is now in Devolutions Server – another grown up feature added to a growing number. In the future there may be SSH support for ephemeral access and push notifications in Devolutions Workspace to enable a dynamic response to check out requests and JIT access.

While still very much a lean SMB PAM platform, there is good flexibility available in the capabilities that buyers can choose from, especially when partnered with the other Devolutions software. Devolutions is gradually adding more enterprise level features which may appeal to larger SMBs. However, there are still no cloud or SaaS options available for PAM, and we would like to see more CIEM, and DevOps capabilities added to the mix – which would be quite compelling given the ease of use already on offer here. And on that note, the promise of a new service to send privileged users to external resources without them interfacing PAM sounds exciting.

Strengths and Challenges

Devolutions has created a compelling line up of software that individually work well to assist with aspects of Remote Access and Privileged Access Management. Together, they provide a good level of wider PAM capability that will appeal to SMBS looking for more than password management. The recent addition of more enterprise PAM capabilities will broaden its appeal to larger SMBs. While many rival vendors have similar capabilities, few have considered the importance of UX design and ease of use to the same degree as Devolutions. This is what sets the software apart from the pack, largely because it was “designed in” from the start. The interoperability of the modules is also a strong point. The remote access capabilities are fine and benefit from Devolutions experience in this increasingly important area of PAM.

The challenge now is for Devolutions to add more capabilities while remaining true to its lean architecture and ease of deployment – no room for bloat. There is great potential to add cloud entitlement capabilities and to offer a SaaS option – perhaps as a combination of appropriate modules. Perhaps the biggest challenge the company faces is not technical but in in its messaging. Currently it is hard for a buyer to determine which products do what and how they might work together from the Devolutions company website. This is a shame because there is the capacity for significant growth at the company if it gets the marketing right.

Strengths

- Good solid PAM solution for SMBs, which understands that sector’s needs
- Ease of use and ease of delivery is a positive for SMBs
- Modules collaborate seamlessly with each other and create numerous options to select and build
- Broad remote access capabilities are top notch and reflect well on the developers
- Strong reporting capabilities of users and accounts
- Private vaults available for end users provide an extra layer of security

Challenges

- Lacks some more advanced PAM features, but this is improving
- On-premises only, no cloud version currently available for modules apart from Devolutions Server
- There is potential in this product, but marketing material could do with clarity to highlight the simplicity of this product, as some notable features are buried in the text

Related Research

Reusable Verified Identity | KuppingerCole

Identity Governance and Administration 2022 | KuppingerCole

Passwordless Authentication | KuppingerCole

CIEM & Dynamic Resource Entitlement & Access Management (DREAM) platforms | KuppingerCole

Zero Trust Network Access | KuppingerCole

Privileged Access Management 2023 | KuppingerCole

About KuppingerCole

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.

Copyright