By Paul Fisher
November 11, 2021

Micro Focus NetIQ Privileged Account Manager

This PAM platform has traditional tools at its core including account discovery, vault, session management and recording. To extend its business usage it also offers effective monitoring, analytics and risk management tools. Privileged Account Manager is described as a gateway approach to privileged access and supports privileged session management across a variety of systems including enterprise business applications such as SAP, major database technologies and popular SaaS applications.

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

Content

1 Introduction

Privileged Access Management (PAM) platforms are cybersecurity components that address the risks associated with the use of privileged access in companies across all sectors. It is recorded that most successful cyber-attacks involve the misuse of privileged accounts, and misuse is enabled by poor management using inadequate PAM software, policies, or processes. Some of the malicious activities that PAM must control are 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.

A 2020 report [1] stated that potentially malicious privileged access from an unknown source accounted for 74% of all privileged access anomaly behaviour detections. So even if the source turns out to be benign, time and resources are spent on verification that would be avoided by an up-to-date PAM installation. It is clear hackers are actively targeting privileged accounts as the best way to get inside an organization and increasingly use them to mount ransomware attacks. Therefore, PAM is an essential component in protecting organizations against cyber-attacks, malware distribution, phishing, and data exfiltration.

Traditionally, privileged accounts were mostly given to administrators who needed access to other user accounts to perform maintenance and upgrade tasks. Some other senior employees may have also been given elevated access rights for specific tasks. This is no longer the case as privilege management use cases extend across entire organizations, with users requiring task-based access to data, services and applications held on legacy and multi- cloud-based infrastructures. And of course, admins still need to perform those traditional privileged tasks!

This change has meant PAM software has developed considerably in the last few years. New and traditional vendors have responded well to demands for more advanced PAM capabilities suitable for the modern computing era.

Interest in Zero Trust Architecture (ZTA) designs and policies has grown. Buyers are increasingly aware that a well configured and up to date PAM platform can be an integral part of any such architecture.

However, the future of business operations will revolve around a new paradigm for highly dynamic IT architecture that melds multiple types of clouds with legacy networks on premises, partner networks and even, in some cases, mainframe installations. This Dynamic Entitlement Resource and Access Management (DREAM) paradigm is what the next iteration of PAM platforms (and other identity and data governance tools) must be engineered to fit; to deliver secure access and greater business value across a new generation of cloud resources.

These ultra-hybrid networks will test existing identity and security frameworks to their limit and call for solutions that provide rapid access to dynamic resources wherever they are held - to where they are required. This is the environment in which Micro Focus NetIQ Privileged Account Manager and other PAM platforms will be deployed into.

2 Product Description

UK based software vendor Micro Focus markets its core PAM platform under the NetIQ brand, a former acquisition, and part of the company's CyberRes security portfolio. Micro Focus is a multi-national business operating in 48 countries with a \$3.0bn annual revenue.

Micro Focus NetIQ Privileged Account Manager has many capabilities that KuppingerCole considers essential if a PAM platform is to meet a wide cross-section of recommended business IT use cases. Its standard features include a credential vault, standard integration with ArcSight SIEM to coalesce privileged user behaviour patterns (as well as other SIEMs that support SYSLOG) with security polices and detect vulnerabilities, privileged session management, session recording and endpoint privileged management.

The platform burnishes these with larger enterprise PAM qualifications with direct connectors to major enterprise applications such as SAP, major databases including Oracle DBMS, Salesforce.com and public cloud services including AWS and Azure. While clearly an enterprise level PAM platform, NetIQ Privilege Account Manager still boasts an easy-to-use interface with a drag and drop process that allows admins to create new rules and policies for privileged access. In addition, a fully integrated testing tool allows new rules to be dry run for accuracy and efficiency before delivered to production.

In recent months, Micro Focus has made efforts to add functionality to its platform, utilizing technical strengths and user experiences from other Micro Focus properties. A good example is the integration of Net IQ Privileged Account Manager with Micro Focus Interset, its proprietary User and Entity Behaviour Analysis (UEBA) solution. We consider this a sensible move and one that will help facilitate planned integration with further NetIQ IAM and IGA products which will allow Net IQ Privileged Account Manager to compete more effectively in multi-hybrid environments.

In a little more detail, Micro Focus Interset can calculate risk scores based on user behaviour anomalies, such as unusual applications accessed, time of day, geographical location, device used and other metrics. NetIQ Privileged Account Manager then uses this information in its decision-making process to provide a privileged session based on the user's risk score. In addition, the package can view recorded keystrokes - although it does not autodetect changes in typing behaviour as some vendors are now offering.

Speed and ease of deployment will be a critical measure for PAM vendors in multi-hybrid environments. Micro Focus has responded with agentless capabilities for both Windows and Linux deployments, requiring fewer components to be installed - increasing efficiency and reducing vulnerability.

Other new features of note include real-time session streaming, for over-the-shoulder monitoring and controls of privileged sessions. This capability allows a secondary user to audit a privileged session in real-time and make decisions based on detected risky behaviour, providing the ability to terminate the session if desired. Such additional human oversight of privileged activity built into the platform will be welcome to those many organizations that are subject to rigorous GRC obligations. Improvements have also been made

to user interfaces across the platform and a new console allows quick toggling between multiple privileged sessions.
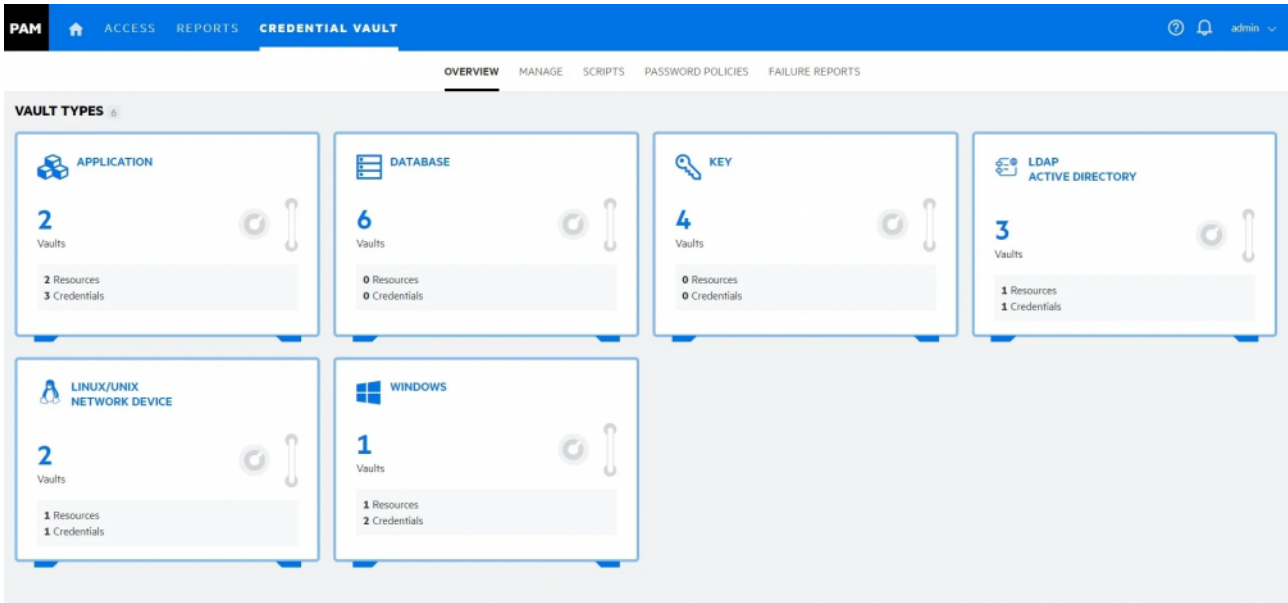

Figure 1: NetIQ Privilege Account Manager benefits from an expressly modern dashboard design. (Source: Micro Focus)

One area we would like to see better addressed is support for DevOps and other agile Ops environments as capabilities remain limited to Ansible scripts available to developers for PAM component deployment, upgrades, and other common use cases in those specialised environments.

As the PAM market starts towards adoption of Cloud Infrastructure Entitlement Management (CIEM) capabilities to assist in multi-hybrid environments as part of a DREAM architecture, we believe Micro Focus has a great opportunity to use its undoubted resources and identity management expertise to accommodate this in its development pipeline. Micro Focus has made a good start by extending privilege escalation to deliver secure programmatic access to cloud, microservices and SaaS applications. NetIQ Privileged Account Manager is now much improved in2021 and better able to compete against the established leaders in the field. The solid and reliable PAM tools at its core: discovery, vault, session management and recording, AAPM, EPM and SIEM are now boosted by proper improvements to Monitoring, Analytics and Risk Management. The continuing alignment with other NetIQ identity technologies can only be a good move as the market shifts towards managing identity and privileged accesses across multi-hybrid operating environments.

NetIQ Privileged Account Manager offers a gateway approach to privileged access and already supports privileged session management across a variety of systems including enterprise business applications such as SAP, databases, and popular SaaS applications. NetIQ Privileged Account Manager would already suit many environments and as future development of advanced and specialist modules now seems assured; it

should be considered by potential buyers from all types of organizations.

3 Strengths and Challenges

Micro Focus has done well to improve the desirability of its PAM platform in recent years and it now sits among the Overall Leaders in the 2021 PAM Leadership Compass and is among the higher rated Challenges in other categories. It has done this by adding some advanced features in areas such as analytics and risk management and is also reaping the benefit of integrating parts of its existing IAM technologies into the PAM platform. This strategy should be developed further to keep pace with rival platforms as it will be key to meeting the PAM challenges within multi-hybrid IT environments.

The company is also remedying the somewhat hotchpotch approach to product delineation and branding by bundling its IAM, Privacy and Security products under the CyberRes line of business. It is still not perfect with those products carrying various names left over from acquisitions, but at least a search for Micro Focus PAM now leads directly to a NetIQ landing page.

We would now like to see greater focus on those areas that would enable NetIQ Privileged Account Manager to move towards the front-rank PAM Leadership. These are of course PAM capabilities designed to be native for DevOps and other agile Ops departments that depend on high availability pipelines, fast access to testing environments and orchestration platforms. The platform already boasts some of the best interface design in the PAM market, so further automation and machine learning capabilities would compliment this well.

Further, Micro Focus should also focus on delivering its planned PAMaaS option and ensure that this utilises the ease of use and advanced features of the existing platform to create a lean, cloud native solution that will appeal, not just to smaller enterprises, but also for individual deployments in very large enterprise frameworks.

![MICRO FOCUS logo]

Strengths

- Good for organizations that already adopt other NetIQ IAM products especially with new family integrations

- Real-time session recoding is now standard

- Support for SAP, database and other enterprise platforms

- Remains a reliable and trusted solution for its basic capabilities but now getting more advanced features on top

- Interface and dashboard design are exemplary

- Financial backing of global enterprise software vendor brings peace of mind to buyer

- Makes good use of in-house IAM expertise from other NetIQ products

- The platform is now positioned to become one of the leading lights in the PAM market with careful development

Challenges

- The product would now benefit from more comprehensive and native DevOps capabilities

- A PAMaaS edition of the platform would be very welcome to SMBs and specialist buyers

- Always on and scheduled account discovery scans are missing

- JIT provisioning requires closer alignment to common DevOps tools

- Micro Focus website remains confusing to buyers and dual branding of identity and security products could impinge on market share and brand awareness in this market

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
Market Compass: Data Governance Platforms -71137
Leadership Brief: Privileged Account Management Considerations - 72016
Leadership Compass: Identity Provisioning - 70949
Leadership Compass: Identity Governance & Administration - 71135
Leadership Compass: Privileged Access Management - 80636

Endnotes

1   Vectra 2020 RSA Conference Edition of the Attacker Behaviour Industry Report