KuppingerCole Report

WHITEPAPER

By Paul Fisher

October 22, 2020

Privileged Access Management solutions for Agile, multi-cloud and DevOps environments

Privileged Access Management (PAM) is an important area of risk management and security for any organization. Privileged accounts have traditionally been given to administrators to access critical data and applications. But changing business practices and upgrades to IT including cloud and other trends has meant that users of privileged accounts have become more numerous and widespread. An area in sharp focus is agile development teams such as DevOps and others that need secure access to privileged resources in the cloud; support for these has become essential to many organizations. Such teams need rapid access to privileged accounts, credentials and protected data, and PAM vendors are responding to this demand.

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

Content

Commissioned by SSH.COM

1 Introduction

Today's organizations need to deliver new services and applications as they modernize operations and upgrade IT infrastructure. Unlike in previous generations, the process of updates is almost constant and deployments across different departments often take place several times a day. The process is mirrored in the creation and improvements made to commercial and third-party software.

The pressure on organizations to develop their IT infrastructures and projects within an automated Continuous Integration and Continuous Delivery framework (CI/CD) is increasing. The directive is from senior management who wish to see improvements in competitiveness through better infrastructure, and IT team leaders looking for boosts in software productivity and efficiency to meet the requirements of senior management. Modern organizations are now an unwieldy mixture of interconnected code and applications including microservices, APIs, desktop apps and mobile apps and to keep all these up to speed requires a constant stream of updates and patches – and the roll out of brand new software projects and products.

One catalyst for this change was the DevOps IT team culture which emerged around 10 years ago to break down the traditional Engineering and Operations silos that existed previously, and which often stalled software development and deployment and introduced errors. It was found that co-operation between the teams helped facilitate the desired continuous development framework as developers became used to agile turnaround and rapid software delivery times and operations also worked more efficiently.

At the same time the same pace of developments is expected of other teams within the organization and some of the same techniques used by DevOps are being applied to other areas – most notable the use of cloud and multi-cloud environments spun up from the use of Cloud Service Providers (CSP) including AWS, Azure, Google and other smaller cloud operators. Many organizations now find themselves wittingly or unwittingly using clouds from different providers - each with different sets of standards for handling authentication to access privileged accounts.

However, organisations focusing only on providing solutions faster and more efficiently by applying the agile approach without having strong security principles baked into their overall software development and operations processes are sooner or later, but inevitably, destined to run into information security problems. For more detail on DevOps and its importance to modern application development see Matthias Reinwarth’s Advisory Note on DevOps, referenced in Further Reading.

Why does this matter?

It matters because those working in these agile, fast turnaround environments, increasingly need privileged

access to specific data sources, applications and other resources that are classified as confidential, and must be kept secure. Today, this will include individual pieces of code, containers, APIs as well as discrete data that may relate to confidential company plans or individuals.

With the pressure to deliver results increasing, those in agile environments may be tempted to take shortcuts and work around less than stringent privileged access controls if they can. They may store locally or share credentials to privileged systems and data or embed them within an application or project files they are working on. The challenge is finding a PAM solution that can work at the pressure and speed that agile people already work to keep secrets secure. It must not get in the way.

2 Highlights

- Conventional PAM solutions for securing DevOps and other agile environments impede the process of collaboration, sharing and trust and hinder business focused results
- A brief history of DevOps and why the culture creates unique challenges for PAM solutions.
- When agile teams feel that their access is being slowed down by infrastructure bottlenecks, they are likely to take short cuts endangering security.
- Security should be transparently embedded into DevOps and agile lifecycles.
- Password less, vault less and JIT options may provide an ideal solution for securing secrets within all agile environments.
- The importance of ephemeral authentication for access to privileged accounts for agile teams and multi-cloud environments.

3 DevOps challenges for PAM

Privileged Access Management solutions have evolved from platforms designed mostly to protect and manage privileged accounts traditionally accessed by system administrators. Today, PAM is expected to be far more flexible in range and provide protection to users needing access to many more privileged accounts which includes DevOps teams that have that most challenging of security demands – uninterrupted and rapid access to essential tools.

DevOps PAM requirements are different from regular PAM

While the need for speed and agile development is unquestionably a benefit to organizations, it can add security vulnerabilities to DevOps operations because of human nature and the temptation to take short cuts to get the job done. If developers feel that their access is being slowed down by infrastructure bottlenecks (as they perceive them), they are likely to take short cuts. But they may feel the same about DevOps focused security controls if they are poorly configured and get in the way. As DevOps people are likely to be assigned access to high value, high risk assets via privileged accounts, then PAM controls need to be modern, flexible, latency free and seamless as possible.

DevOps was a kind of revolution in IT because it focused on people and a change in culture to get things done as much as technology.

We should not assume that it is always legacy IT architecture or rusty hardware stacks that can cause this problem for DevOps or other users of privileged accounts - poorly configured cloud infrastructures can also be a problem. According to SSH.COM, a recent survey of 600 IT professionals revealed that 80% considered multi-cloud infrastructures to be a problem for privileged account users.

DevOps was a kind of revolution in IT because it focused on people and a change in development culture to get things done as much as technology. Today, organizations appreciate that good DevOps people are of great value to the business, so they need to be looked after and, pertinent to this report, they need to have security tools that do not impede them from creating value. A people focused, enabling security culture is more likely to keep key employees happy and how PAM is implemented across the DevOps powered CI/CD lifecycle will play a crucial role in this.

Key factors in delivering modern PAM to DevOps teams

1. DevOps is full of secrets and stuff that is pure gold to cybercriminals: usernames, passwords, credentials API tokens, SSL certificates, SSH keys, runtime environments, containers, microservices

and more. As these are all high value items, DevOps is fast becoming a prime attack vector.

2. Collaboration, sharing, and trust are crucial to successful DevOps. PAM for DevOps must not impede the process of collaboration, sharing and trust.
3. DevOps people may have gotten used to taking shortcuts to assign privileged access to each other. PAM for DevOps must provide the same ease of access but in a secure transparent manner that does not become a bottleneck in the DevOps lifecycle.
4. PAM for DevOps must be capable of efficient Application to Application Privileged Management (AAPM) for containers and other non-human devices that require privileged access. Some containers may even have access to privileged accounts embedded in code.
5. Well managed DevOps teams collect and analyse data on testing, deployment, output, failure rate etc to improve performance. If possible, PAM should gain access to such data to fine tune privileged access for DevOps to match the goals of DevOps.
6. DevOps people spin up and spin down multi-cloud services and resources all day long. Any PAM solution must be able to deal with this functionality natively while also managing those DevOps operations that, for whatever reason, are carried out on-premises.

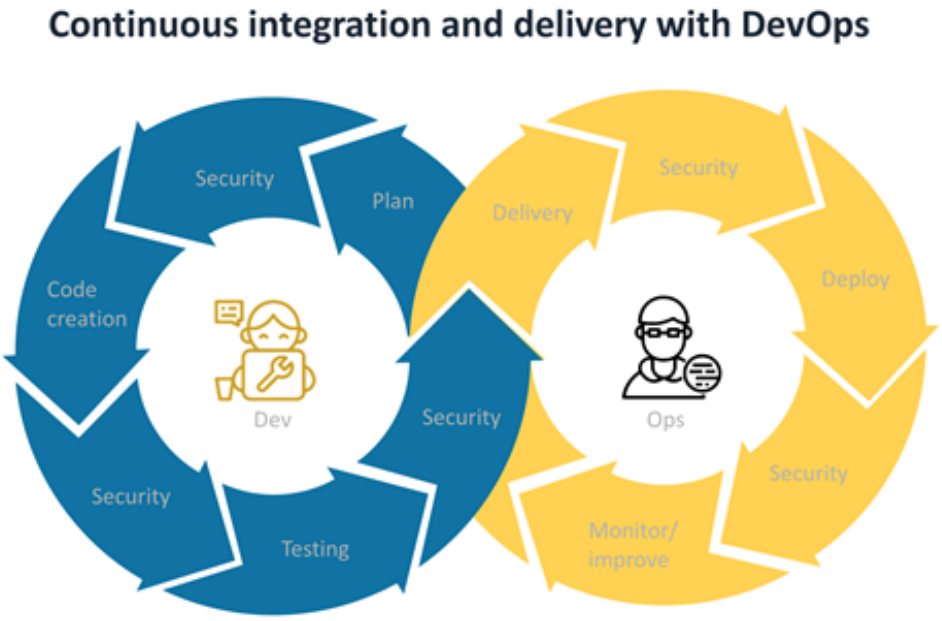

Figure 1: Transparent Security platforms including PAM must be embedded within the CI/CD lifecycle. A security feedback mechanism is also advisable to allow DevOps and other agile development teams to act quickly on vulnerabilities as they arise.

4 Finding the right PAM platform for agile teams using multi-cloud environments

The demands of agile teams are different from conventional IT environments and they are voracious users of privileged accounts to access high value digital assets. The expectations are for teams to deliver and so they may take short cuts, to get the job done. However, organizations have a corporate duty to protect privileged accounts wherever they exist in the organization for the good of all for agile development teams in multi-cloud environments.

For PAM to work in agile environments successfully it needs to deliver in four key areas:

1. It must be lean, scalable, and flexible enough to work alongside agile teams
2. It must be cloud agnostic and able to operate consistently on all the cloud platforms that agile teams favour
3. It should not be solely reliant on passwords and vaults
4. It should be compatible with ephemeral and just-in-time (JIT) authentication tools

Scalability

Teams are under pressure to deliver on demand and to ensure that what they deliver is robust enough to fit organization demands as they change – often daily. The scalability also applies to internal resources as projects change and new demands must be met, and changes made to already deployed applications – right throughout the continuous life cycle (CI/CD). A PAM platform must scale in tandem with the needs of agile teams and cloud deployment without friction.

Native platform support

For best advantage and for PAM to be able to keep pace with the speed of agile teams, it should ideally run agnostically in the cloud environments that DevOps teams use to get the job done. PAM should also be compatible with container orchestration services such as Kubernetes and other popular development tools. The problem arises when running different clouds each with their own native requirements

Non-reliance on passwords and vaults

While PAM can use traditional password and vault mechanisms, for maximum efficiency and ease of use it is highly recommended that faster environments benefit from the vault-free and password-less PAM platforms that are now being developed as these remove security bottlenecks in the process.

Ephemeral and JIT based authentication

To enable scale and fast turnaround, and to replace passwords, PAM for should support ephemeral authentication techniques and JIT access so that privileged accounts are used one time only and there is no danger of access left open in orphan accounts, creating a security risk.

Technologies and practices that can help secure agile development

Vendors in the PAM space are looking at various technologies that serve the needs of agile people and team management. Some vendors are looking at new ways to manage passwords and credentials in PAM solutions by using API calls to connect to passwords held in a vault. The API calls process credential and password requests. While this process addresses the speed issues through automation of traditional vault technology it does not replace passwords, nor does it address credentials hard coded into containers or applications. Also, it does not have JIT as its default authentication protocol.

Other vendors may suggest best practice security methods for applying security in agile teams while still relying on passwords, vaults, and password management tools. This is akin to expecting end users to bend to old PAM rules rather than applying PAM to work the way user need. Some vendors are using more specialised third-party versions of the traditional vault to embed in targeted editions of their platforms – such vaults will store tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data.

Such vaults are often more tuned to the needs of DevOps and other agile environments in the capacity of secrets they hold and can be created very quickly and manged through HTTPS or CLI. Deployment of a third-party vault is useful in hybrid PAM architectures where DevOps may be manged by its own dedicated PAM solution. While this approach fulfils some of the needs of DevOps it still does not necessarily reduce reliance on conventional password-based PAM architectures. Making PAM solutions compatible with well-known tools such as Kubernetes, Ansible, Jenkins is also happening, and this is obviously a good move.

There are now solutions that have addressed the vault and password issue and are now offering PAM for *agile teams* that rely on JIT access using some form of ephemeral authentications process that is one time only, does not need to store passwords and relies on keys to authenticate. Such solutions potentially offer the solution to providing the security and convenience that fast-paced environments crave.

Finally, some vendors do not have a specific agile focused solution and rely on best practice tips and marketing which do not necessarily get to grips or understand the needs of DevOps to make out their solutions is tuned for.

5 Cloud-based challenges for agile teams using privileged access

Teams involved in agile projects of all kinds will also need access to resources and increasingly these are accessed to and from cloud and multi-cloud and hybrid environments. Such users also present challenges to traditional methods of privileged access management, often around scoping what relevant data exists in the cloud, building applications in the cloud, should be made privileged and preventing privilege creep in these multi cloud environments.

Other teams in modern organizations also work in agile ways to get projects completed and these can be from all lines of business including HR, Finance, creative teams, in-house startups and other teams employing the agile methodology.

Creating and storing passwords for these accounts in a vault is also a challenge as new requests for access will appear all the time - making it difficult for administrators to keep up. It is not impossible, but it would put a strain on the PAM platform and agile teams may lose patience and once again, revert to cutting corners.

Organizations are using Tier 1 Cloud Service Providers (CSP) such as AWS or Azure or smaller cloud resellers to spin up development, frameworks, and workloads to test and deploy projects.

More often, organizations are using Tier 1 Cloud Service Providers (CSP) such as AWS or Azure or smaller cloud resellers to spin up development, frameworks and workloads to test and deploy projects, often in multi-cloud environments with mixed cloud providers. However, the native environments of the different cloud providers do not protect privileged accounts as best they can. There are several problems and challenges here:

All CSPs are different, with different technologies and no common domain

- Roles are assigned differently across various CSPs (for example, AWS roles are different from GCP roles) and both the access admins and privileged users need to be trained per CSP tool
- Tracking and auditing sessions needs to be done in separate systems
- Every CSP has a slightly different approach to how they develop their services and the update lifecycle is different. Ensuring that the access configurations and levels of privilege are up-to-date per CSP tool is a big and a complex task

Accounts and entitlements can be defined and generated from multiple sources

- Dynamic discovery of cloud assets per CSP tool falls short of proper oversight, since the organization is missing a centralized view of the global cloud estate
- Onboarding, change management and offboarding users per CSP tool is a lot of work

Mixing permanent credentials and cloud services that are ephemeral by nature

- Cloud instances are spun up and down at a rapid pace, there are multiple privileged roles with various levels of privilege per task, protocols might be different per target host, and third parties and partners should often have only temporary access to target.
- This mix of variables makes it hard to reliably track, grant, revoke and manage access using traditional, permanent credentials and audit every session with the right identity

Privileged access through CSP consoles often leads to privilege creep

- If privileged access is managed using separate CSP native tools, there is the temptation to grant excessive and broad privileges just to expedite the process.
- There is also a pressure to share credentials and disregard proper segregation of duties ‘to get the job done’, especially in DevOps and other fast-paced coding environments

If the infrastructure is concentrated, a single misconfigured entitlement can lead to a massive exposure

- A significant part of a company’s infrastructure might be under the jurisdiction of a single cloud account. This means that a single misconfigured privileged account entitlement might lead to a situation where a considerable part of the infrastructure is broken or stolen, affecting hundreds of flies and servers.

CSPs offer a multitude of interfaces for interaction, such as consoles, CLI clients and SDKs

- Cloud platforms are accessible using many means that allow the user to perform very different operations on the platform.

6 SSH.COM PrivX for hybrid environments

SSH.COM is a security technology company based in Helsinki, Finland. It was founded in 1995 by Tatu Ylönen, the inventor of the Secure Shell protocol (SSH). It currently has more than 3000 customers in Europe, North America, and Asia. The company sells PrivX as its main offering in the PAM market, which offers a vaultless, password free option for DevOps environments.

SSH.COM has a good point when it says that the Secure Shell Protocol is deeply immersed in DevOps and agile operations practice and enables the rapid and highly automated build and release process. This is one of the reasons why PrivX offers an alternative to conventional shared account password management technology.

PrivX is a PAM solution that supports the theory that storing credentials and passwords is bad practice, even in a vault, and especially in the cloud native environments that DevOps operates. PrivX operates primarily without a vault or permanent credentials. Instead, it establishes a trust relationship between the target server environment and itself by acting as a certificate authority for all SSH and RDP (and HTTPS) access. PrivX then authenticates users with one-time ephemeral certificates that exist long enough to establish the connection and then automatically expire after the authentication.

Privileged users do not handle or see any privileged credentials or passwords during the process, nor are there any credentials left behind in the environment that would need to be vaulted – or could be shared or misused. All access is granted on-demand and is temporary in nature by default.

The preferred Just in Time Approach (JIT) to PAM means that it is easier to control access in DevOps where access demands change rapidly among changing groups of users, applications and machines and eliminates the need for permanent privilege accounts that grant users always available access and can be a security risk. It means that DevOps does not need a separate Privilege Escalation tool as all access is granted on a one-time basis with the level of access determined at time of request based on the role of the DevOps team member.

However, since many companies cannot adopt „the password less paradigm“ overnight, for contexts where ephemeral, just-in-time authentication is not possible, the solution is equipped with a vault for storing secrets – which the users also never see or handle.

Storing credentials and passwords is bad practice, even in a vault, and especially in the cloud native environments that DevOps operates.

PrivX can auto-discover multi-cloud resources making them accessible when onboarding from a single dashboard. Remote sessions are supported through standard web browsers and privileged users can

connect to their required files and services via SSH and other standard protocols, as well as Web apps. Users can also connect to target hosts using the SSH & RDP clients installed on Windows, Linux or Mac workstations as an alternate method to the PrivX GUI, giving extra flexibility to DevOps and the way it may prefer to operate.

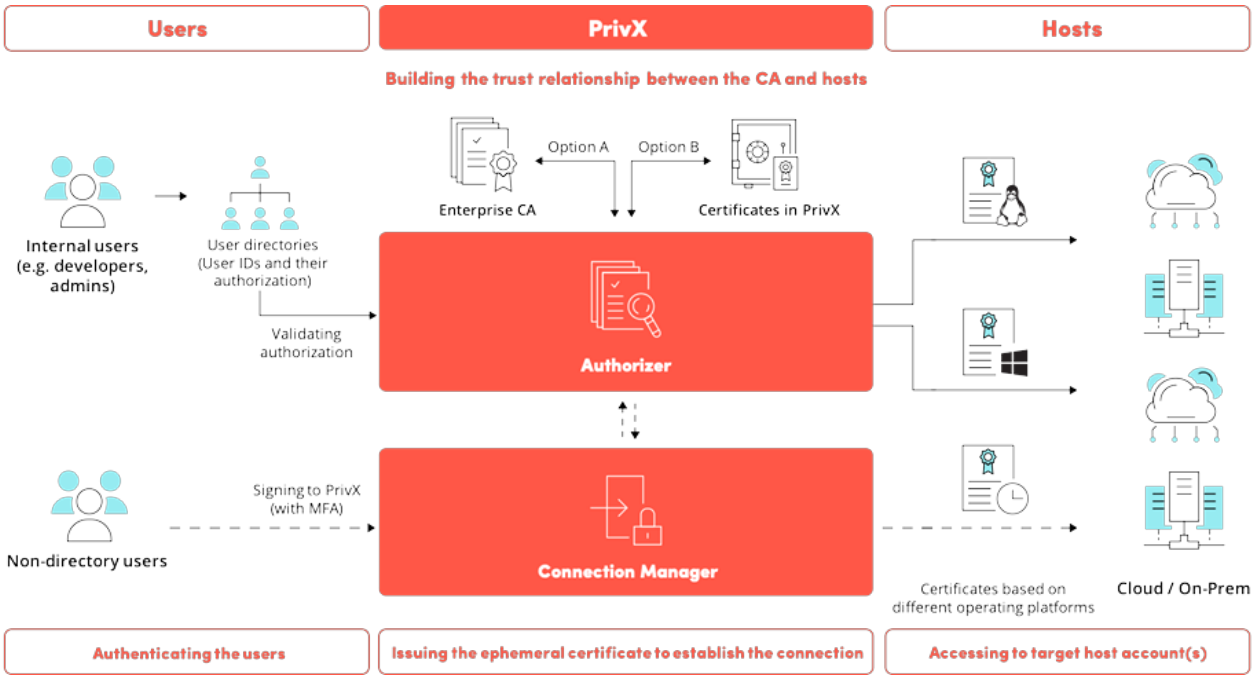

Figure 2: SSH.COM can process internal users and non-directory users with JIT certificate-based authorization and authentication. Certificates are issued for both types to access multiple servers. (Source: SSH.COM)

While Just in Time and ephemeral access is ideal for DevOps end goal of rapidly deploying code and building applications, managers must ensure that compliance is not forgotten in the process. DevOps must still be accountable. Therefore, administrators or whoever may be responsible for managing privileged access can gain visibility to ongoing sessions on a single dashboard & terminate them if needed. Further, all sessions can be recorded and by integrating a compatible third-party Security Incident & Event Management (SIEM) platform or cloud-based log collectors (Cloudwatch, Event Hubs), alerts can be issued based on audited events. All SSH logs can be indexed and made searchable to aid investigations and security forensics.

Privileged users log into a clean looking browser-based interface via Single Sign On (SSO) and can see what resources they can access based on their current role and click though appropriately.

There is support for federating users from Microsoft AD/LDAP, Azure AD, Google Suite, Amazon Cognito or any OpenID Connect Provider and these stay in sync as roles change. Keeping track of users across the

organization is facilitated by the dashboards. Sessions can also be observed in real time with alerts generated for anomalous behavior.

Privileged users log into a clean looking browser-based interface via Single Sign On (SSO) and can see what resources they can access based on their current role and click though appropriately. Access rights are automatically updated as roles change in in either AD, LDAP or OpenID directories or from IAM system that work with PrivX including OneLogin, Okta, ForgeRock and Ubisecure. PrivX can scale from supporting dozens of hosts to managing access to full-scale enterprise environments.

It is no surprise that SSH.COM would consider its solution ideal for today's complex operating environments. It presents a unique approach for managing certificate based SSH and RDP access by offering a certificate authority to issue ephemeral one-time access credentials. SSH.COM appeals to organizations that either need a vault-less approach to manage RDP and SSH access with basic PSM capabilities or are looking to complement their existing PAM solution with these features. PrivX is by its nature ideal for DevOps teams looking for privileged access with ephemeral certificate delivery at its core. But its ability to override the native requirements of so many cloud environments through its certificate-based technology is even more compelling.

7 Recommendations

Even if we lived in a world without cyber-attacks, the efficiency, and operational benefits that a well set up PAM solution delivers should be attractive to any business. DevOps and agile operations in multi-cloud environments present new challenges to protecting privileged accounts and it changes the rules on what is a privileged account and asks questions of the more static nature of those PAM solutions that are designed for conventional operating environments.

If an organization depends on agile teams, it is essential the access and the secrets generated by those teams are secure and easily available. However, many existing PAM solutions are simply too comprehensive for the specialist needs of agile operations and due to their reliance on passwords and vaults do not necessarily meet the operating speed requirements.

This does not mean that many PAM solutions cannot provide security– they certainly can – but they might deliver at a cost to the speed, flexibility and reliability that agile environments rely on. Some vendors are thinking about these teams s by designing new vaults or better management tools – but again these do not necessarily address the heart of the issues outlined in this whitepaper.

Five steps to securing DevOps and other agile users with PAM

1. Vigorously assess security and compliance risks of any existing or proposed PAM solution for to determine fitness for purpose.
2. Do not assume that an existing PAM solution will automatically cope with the specialist operational and security challenges of agile teams.
3. Consider a hybrid PAM solution with a dedicated PAM solution for agile teams across the organization running alongside any legacy PAM platform
4. Ensure that the PAM platform does not impede the culture, efficiency, and business benefits of agile development.
5. Continuously monitor PAM to discover potential bottlenecks and vulnerabilities that undermine security.

What kind of solution is chosen will depend heavily on the importance of the agile teams within an organization and if the culture fostered is echoed throughout the organizations If the organization has signed up to CI/CD being the driver of its digital transformation it would make sense to select a PAM solution that fulfils security without in any way impeding the culture.

Do not upset the agile success story – its prime goal is the development and delivery of projects – not to worry about security or stuff that is “not their department”. Even if the organization already has a PAM platform in place, the principals of a hybrid PAM architecture should be considered so that agile ops has a dedicated and custom PAM solution in place, especially when using multi cloud environments.

However, it must not be forgotten is still part of the organization and cannot be left unchecked even if its secrets are secured, therefore any PAM solution must also fulfill compliance demands whether integrated, validated through robust add on modules or via trusted third party platforms.

8 Related Research

Advisory Note: Eight Fundamentals for Digital Risk Mitigation in the Age of Transformation – 71302
Advisory Note: Integrating Security into an Agile DevOps Paradigm – 71125
Architecture Blueprint: Access Governance and Privilege Management - 79045
Architecture Blueprint: Identity and Access Management – 72550
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 Identity-Based Computing
Leadership Brief: Privileged Account Management Considerations – 72016
Leadership Compass: Access Controls Tools for SAP Environment – 80104
Leadership Compass: Identity Provisioning – 70949
Leadership Compass: Identity Governance & Administration – 71135
Leadership Compass: Privileged Access Management - 79014

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.