KuppingerCole Report

WHITEPAPER

by Matthias Reinwarth| March 2019

PATECCO Privileged Access Management Services

Privilege Management is the set of critical cybersecurity controls that deal with the management of security risks associated with privileged access in an organization. Maintaining control over privileged users, extended privileges and shared accounts demands for a well-integrated solution, consisting of risk mitigation, well-defined processes und well-executed implementation.

by **Matthias Reinwarth**
mr@kuppingercole.com
March 2019

Commissioned by PATECCO

KuppingerCole Whitepaper
Privileged Access Management PATECCO
Report No.: **80037**

Content

Related Research

Architecture Blueprint: Access Governance and Privilege Management - 79045
Advisory Note: How to Assure Cloud Services - 72563
Leadership Compass: Adaptive Authentication - 79011
Leadership Compass: Privilege Management - 72330 (update pending)
KuppingerCole Hot Topic Area Privilege Management

1 Introduction

Traditionally, the management of identities and their access to IT systems within an organization have been split up within different disciplines. Business users, the so-called standard users, have been managed within the traditional Identity and Access Management (IAM) systems and have been more recently covered within Access Governance and access analytics systems. Privileged Access Management (PAM) is the term for technologies that manage administrative accounts, that help monitor and limit elevated rights and support in managing shared accounts. In the past, Privilege Management developed out of the management of shared accounts and passwords.

In recent years, the perception of privilege management has changed considerably. Various vendors have significantly expanded their offerings, while various acquisitions have also resulted in infrastructure vendors offering a broader product portfolio and evolving from specialized niche vendors to market leaders. Within the last 5 to 10 years Privilege Management has been added to the portfolio of identity and access capabilities provided by IAM, Corporate Governance or Security teams.

Why should an attacker be satisfied with taking over the account of a regular user if he can instead take over entire segments of an IT infrastructure as an illegitimate administrator?

Managing privileged users or, as KuppingerCole refers to it, Privilege Management, is a significant undertaking for an organization. An insider is often more knowledgeable and aware of the business' process and technical landscape. And if an insider account gets hijacked, the outsider has the same opportunities for attacking. The malicious insider (or the hijacked one) with privileged credentials can cause significant damage including, but not limited to:

- Delete, modify or read all email and other communication records;
- View or modify salary records of all employees;
- Leak of intellectual property;
- Share confidential data, including personal information, with shareholders or hacktivists.

But it is not only threats that have changed and increased. The last decade has seen significant changes in business requirements and IT. Business models have changed, the ubiquitous digitalization has completely transformed enterprises, their networks and their application infrastructure. New infrastructure concepts in the cloud, delivered as infrastructure as a service, up to completely new offerings through business-software as a service create a multitude of new administrative accounts. New applications and platforms based on mobile devices create new work concepts and business models on the one hand, and present IAM and Privilege Management with new challenges on the other.

In a time of increasing numbers of cyber-attacks and data breaches, it is obvious that these incidents are related to privileged user accounts. In addition, analyses of the latest security incidents suggest that large scale data theft is likely to be caused by users with elevated privileges, typically administrative users. So, it's not surprising that privilege management is not just an issue that executives (CIOs and CISOs) have to deal with but is increasingly an area that auditors and regulators have to put on the agenda. In positive terms, the impact of privilege management (and therefore the benefits of investing in this area) on overall risk mitigation is exceptionally high compared to other types of IT and security technologies.

Privileged Access Management represents the set of critical cybersecurity controls that deal with the management of security risks associated with privileged access in an organization.

This white paper describes how Privilege Access Management is integrated into a comprehensive IAM architecture. It provides an overview of essential components and current enhancements and trends in this area. The final section shows the importance of an adequate implementation of Privileged Access Management in a user company, exemplified by the consulting activities of PATECCO and its range of services.

2 Highlights

- Provides the KuppingerCole definition of Privileged Access Management.
- Shows the integration of Privileged Access Management into an overall IAM architecture
- Identifies the key customer challenges which lead to the rise of Privileged Access Management as a key topic for the Information Security organizations.
- Describes common features found in Privileged Access Management products.
- Looks at the organizational prerequisites for successful deployments of Privilege Access Management.
- Gives an overview of the services provided by PATECCO for executing successful Privilege Access Management projects and delivering sustainable PAM solutions.

3 Approaching Privileged Access Management from an Architecture Perspective

Privileged Access Management tools are designed to address scenarios such as use of shared accounts, monitoring of privileged activities and controlled elevation of access privileges. A consistent implementation for the fulfilment of these requirements must be reflected in an appropriate architecture, which in turn must represent a valid portion of an overall IAM architecture.

The KuppingerCole IAM/IAG Reference Architecture provides a comprehensive and evolving foundation for deriving and implementing standardized, yet adequately tailored IAM/IAG architectures integrated into an overall enterprise architecture. It is rooted on a fundamental architectural distinction between four high level capability areas.

These include:

- Administration
- Audit & Analytics
- Authentication
- Authorization

Building on this premise, a set of discrete architectural IAM components is assigned to one or more of these capability areas. Thus, a complete, comprehensible and flexible overall architecture can be achieved.

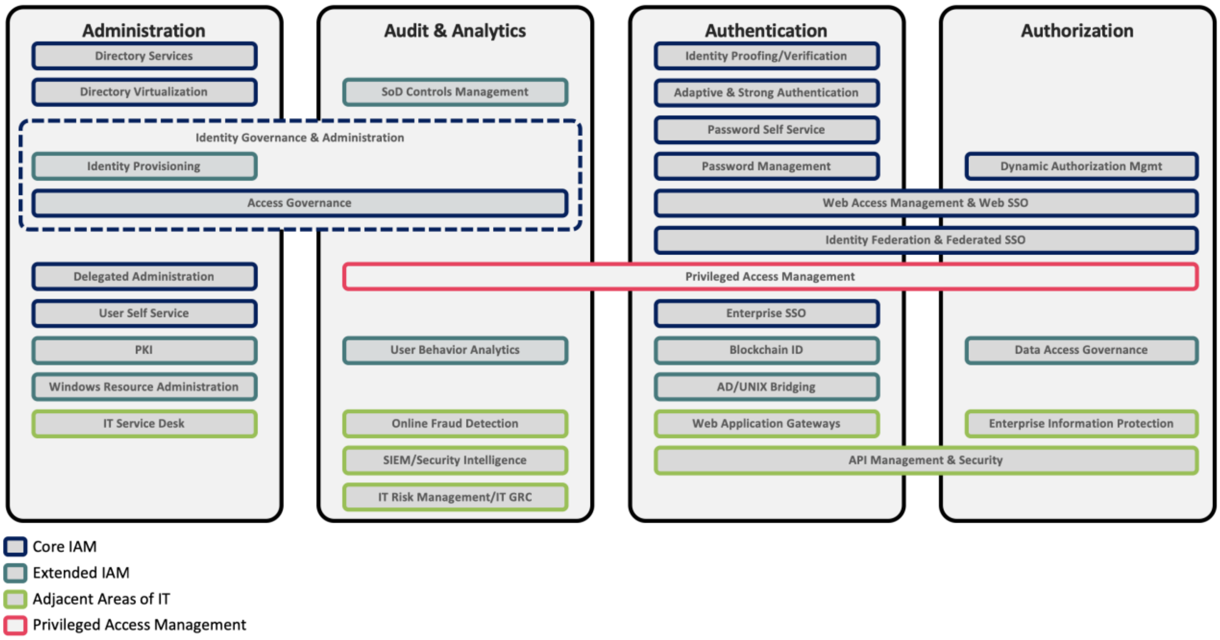

Figure 1: Privileged Access Management as part of the KuppingerCole IAM / IAG Reference Architecture

The building blocks are categorized as

- indispensable (Core IAM),
- complementary (Extended IAM) and
- peripheral (Adjacent Areas of IT),

which anticipates an efficient conceptual anchoring of the IAM / IAG architecture in a comprehensive enterprise architecture.

The given structure, the localization of building blocks within capability areas and the categorization related to a mature enterprise architecture landscape provide both conceptual guidance as well as the required degrees of freedom in designing, verifying and assessing system and process landscapes for IAM / IAG and related architectural areas.

PAM has emerged as one of the most crucial IAM technologies that have a direct relevance and impact on an organization's cybersecurity program.

Privileged Access Management over the past few years, has become one of the most relevant areas of Cyber Security associated with Identity and Access Management that deals with identifying, securing and managing privileged credentials across an Organization's IT environment. Once considered a technology option for optimizing administrative efficiency by managing passwords and other secrets, PAM has evolved into a set of crucial technologies for preventing security breaches and credential thefts. PAM today concerns Security and Risk Management leaders as well as Infrastructure and Operation (I&O) leaders across the industries for several security and operational benefits.

This is clearly reflected in the fact that Privilege Access Management spans three of the four high level capability areas. PAMs capabilities are directly associated with the areas "Audit & Analytics", "Authentication" and "Authorization". Of course, PAM is also highly dependent on administrative capabilities, i.e. the fourth high level capability area. These functions and services are typically located outside the core PAM capabilities and are covered by "Identity Provisioning", "Access Governance", "User Self Service" and "Delegated Administration" for privileged accounts and their entitlements.

In this context it is important to clearly define which module takes on which task: The provisioning of unique and trusted identities in the IAM is an indispensable foundation. However, this function is being provided by the Directory Services Building Block as part of the entire reference architecture. These identities are assigned permissions by managers and through life cycle processes in an Access Management system. At the same time, elevated privileges are granted and managed through separate Privilege Management interfaces and can be associated with distinct identities.

For this purpose, clearly defined technical interfaces are required that match information about assigned permissions from Privilege Management against authoritative IAM systems. Therefore, it is necessary to collect or have immediate access to privileged user account, group and access data from the Privilege Management System.

Ideally the Privilege Management infrastructure can be considered as a highly specialized target system for the Access Management and Access Governance infrastructure, allowing it to provision, recertify and revoke elevated access to and from IT systems.

4 Privileged Access Management Solution: Functionalities and Capabilities

Privileged Access Management represents the set of critical cybersecurity controls that address the security risks associated with privileged users and privileged access in an organization. The privileged nature of these accounts provides their users with an unrestricted and often unmonitored access across the organization's IT assets.

This does not only violate basic security principles such as least privilege but also severely limits the ability to establish individual accountability for privileged activities. Privileged accounts pose significant threat to the overall security posture of an organization because of their heightened level of access to sensitive data and critical operations. Security leaders therefore need stronger emphasis on identifying and managing these accounts to prevent the security risks emanating from their misuse.

Privileged Access Management tools are designed to address these scenarios by offering specialized techniques and process controls, thereby significantly enhancing the protection of an organization's digital assets by preventing misuse of privileged access.

4.1 Basic and advanced PAM capabilities

Core functionalities of PAM tools include

- Credential vaulting
  Technology and processes for the secure, audited storage of and access to passwords and similar cryptographic key material.
- Password rotation
  the reduction of the lifespan of passwords by changing it frequently to reduce the risk of compromise, especially for critical accounts.

But more advanced capabilities such as privileged user analytics, risk-based session monitoring and advanced threat protection are becoming the new norm. With the attack surface expanding and the number and sophistication of attacks increasing every year, an integrated and more comprehensive PAM solution is required – one that can automatically detect unusual behavior and initiate automated mitigations.

Among the key challenges that drive the need for managing privileged access 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, and
- Accidental misuse of elevated privileges by users

PAM has become an important digital risk management discipline that helps security leaders with controls essential for securing privileged access to data, applications and infrastructure.

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
- Identification and continuous tracking of ownership of privileged accounts throughout their life-cycle
- Establishing and managing privileged session to target systems for enhanced operational efficiency of administrators
- Auditing, recording and monitoring of privileged activities for regulatory compliance
- Managing and monitoring administrative access of IT outsourcing vendors and MSPs to internal IT systems, and
- Managing and monitoring privileged access of business users and IT administrators to cloud infrastructure and applications

4.2 Building blocks for PAM deployments

The following technologies and tools are important building blocks of today's Privileged Access Management solutions. Depending on individual requirements and the chosen vendor(s) they typically form the foundation of a real-life PAM architecture.

Shared Account Password Management (SAPM): Shared Account Password Management offers technology to securely manage privileged credentials including system accounts, service accounts or application accounts that are generally shared in nature. At the core of SAPM products is an encrypted and hardened password vault for storing passwords, keys and other privileged credentials for a controlled, audited and policy-driven release and update.

Privileged Session Management (PSM): Privileged Session Management offers the technology to establish a privileged session to target systems including basic auditing and monitoring of privileged activities. PSM tools also offer authentication, authorization and Single Sign-On (SSO) to the target systems.

Application-to-Application Password Management (AAPM): AAPM is an extension of SAPM tools to manage accounts used by an applications or systems to communicate with other applications or systems (such as databases etc.). AAPM tools offer elimination of hardcoded credentials in application code, scripts and other configuration files by offering a mechanism (generally APIs) to make credentials securely available when requested.

Session Recording and Monitoring (SRM): SRM is an extension of PSM tools to offer advanced auditing, monitoring and review of privileged activities during a privileged session, including but not limited to key-stroke logging, video session recording, screen scraping, OCR translation and other session monitoring techniques.

Controlled Privilege Elevation and Delegation Management (CPEDM): Technology that deals with controlled elevation and policy-based delegation of a users' privileges to super-user privileges for administrative purposes.

Privileged User Behavior Analytics (PUBA): PUBA uses data analytic techniques to detect threats based on anomalous behavior against established behavioral profiles of administrative users as well as user groups and administrator roles.

Privilege Account Discovery and Lifecycle Management (PADLM): This deals with discovery mechanism to identify shared accounts, software accounts, service accounts and other unencrypted/ clear-text credentials across the IT infrastructure. PADLM tools offer workflow capabilities to identify and track the account's business and technical ownership throughout its lifecycle and can detect changes in its state to invoke notification and necessary remedial actions.

Endpoint Privilege Management (EPM): EPM offers capabilities to manage threats associated with local administrative rights on windows, mac or other endpoints. EPM tools essentially offer controlled and monitored escalation of user's privileges on endpoints and include capabilities such as application whitelisting for endpoint protection. Categorically, we define EPM solutions to primarily offer three distinct technologies:

a. **Application Control**: This allows organizations to control what applications can be allowed to run on an endpoint. This is usually achieved through application whitelisting in which only known good applications are placed on a pre-approved list and are allowed to run. Application control provides effective protection against shadow IT challenges for organizations.
b. **Sandboxing**: This technology uses the approach to isolate the execution of unknown applications or programs by restricting the resources they can access (for eg., files, registries etc.). This technology, also known as application isolation, provides an effective protection against cyberattacks by confining the execution of malicious programs and limiting their means to cause the harm.
c. **Privilege Management:** This technology encompasses user and application privilege management. For user privileged management, it deals with controlled and monitored elevation to local admin privileges. Application privilege management deals with exception or policy-based elevation of administrative rights for known and approved applications to execute successfully.

Privileged Access Governance (PAG): PAG deals with offering valuable insights related to the state of privileged access necessary to support decision making process. PAG includes privileged access certifications and provisions for customizable reporting and dashboarding.

4.3 Defining individual PAM landscapes

Regardless of the tool decision, the most important points are that Privilege Management is not mainly seen as a technical issue and that the customer challenges of Privilege Management are covered at all – the worst thing is to further ignore or underestimate the challenges which lead to the rise of Privilege Access Management. Therefore, the first step to Privilege Management is not selecting the tool but doing the homework on the organizational side.

Reducing the overall number of privileged accounts, limiting accounts to only the access rights that are essentially required and even consolidating IT platforms might help reducing the exposure of critical accounts. This includes taking into account all regulatory requirement and the legal requirements

The criticality of privileged accounts, which makes a PAM solution necessary, inevitably makes the appropriate execution of such an essential and security-relevant deployment project a highly critical task in turn.

5 PATECCO Services for implementing Privileged Access Management solutions

Access to the resources and competencies of an experienced service provider can accelerate the implementation of a PAM project and its integration into an enterprise IT infrastructure. By deploying best practices and access to proven project procedures, clearly defined project goals can be achieved quickly.

PATECCO is a privately held company providing services in the areas of the development, implementation and support of Identity & Access Management solutions. PATECCO is based in Bochum, Germany, with a branch in Sofia, Bulgaria. PATECCO is a highly experienced player in the field of IAM with over 20 years of experience. The services offered go well beyond traditional on-premises IAM and cover Cloud Access Control, Access Governance, RBAC, SIEM, PKI. PATECCO provides managed services for IAM solutions as well, with PAM being also on the roadmap for managed services.

Privileged Access Management as an essential discipline of IAM as well as a separate offering adds to the company's portfolio of value-added services for customers of different sizes from industries such as banking, insurance, chemistry, pharma and utility. They have successfully executed various large-scale PAM projects with major enterprises in the finance and the telecommunications sector. The focus of their current service offerings lies on their main locations, Germany and Bulgaria.

The following sections provide an overview of typical relevant phases of a PAM project for the introduction of an enterprise-wide Privileged Access Management solution according to the standard procedure of PATECCO.

5.1 Gathering requirements

Being vendor neutral, PATECCO is in a good position to assist customers in shaping and scoping the overall PAM target landscape. Selecting the appropriate building blocks from the functions and technologies described in the previous chapter is the first import step, followed by an adequate design of the target architecture and the required processes and workflows. This is achieved by gathering information about the individual requirements of the customer organization.

The questionnaire deployed for these purposes covers various aspects of the processes, the technical landscape and the policy framework in place. This clearly reflects best practices also recommended by KuppingerCole: The first step to Privilege Management is not selecting the tool but doing the homework on the organizational side.

5.2 Identity Consolidation

The management of privileged identities and their access to critical systems only makes sense if all identities that are to be managed are unambiguously recorded in the context of an initial survey. For this reason, PATECCO recommends starting a PAM project with an analysis, cleansing and consolidation of existing identities, roles, permissions and local accounts across all, especially heterogeneous, resources.

Only if a uniform and unambiguous collection of all these identities is guaranteed, the next step can be taken meaningfully regarding the consideration of privileged access. Specifically, this means that all identities can also log into the system in a personalized manner, so that authorizations can then be granted to this unique identity even in administrative systems.

Unique, reliable identities, accounts, roles and well-defined permissions on a "least-privilege" basis are a mandatory prerequisite for the start of a successful PAM implementation.

As best practices from the PATECCO project experience, an Active Directory is used to consolidate UNIX, Linux, and LDAP identities with a single, unique ID for centralized identity, role, and permission management and for Kerberos-based authentication.

When determining the privileged accounts to be managed on this basis, a cleanup is also useful and necessary: only accounts that are actually required may be managed and their authorizations should be reduced to a minimum. Unnecessary privileged accounts can and should be deleted or at least deactivated. Local (Windows) administrators are often overlooked, but in an appropriate management concept they should also be considered with their own proper lifecycle.

5.3 Privileged Access Request

The central challenge for any privileged access management system is the use of a (minimum) four-eyes principle that uniquely identifies the requestor and the approver and enables subsequent traceability. A workflow-based request and approval mechanism for privileged access is usually used for this purpose.

Access to and use of privileged accounts is a key focus for regulators in many industries, but access to critical corporate resources should also be controlled, documented, and monitored in every other organization to improve security, governance, and compliance.

5.4 Super User Privilege Management (SUPM)

PATECCO calls the ability to enable a "least privilege" access model for authorized users via authorization extension tools SUPM, Super User Privilege Management. The aim of this procedure, which KuppingerCole refers to as Controlled Privilege Elevation and Delegation Management (CPEDM), is to assign only the minimum set of authorizations at session runtime. An interactive session starts with as few authorizations as possible and is only elevated when required. In particular, the aim is to avoid the necessity of accessing shared accounts through a modified authorization model.

For this PATECCO uses the combination with Identity Consolidation in Active Directory. This provides further administrative advantages so that roles and authorizations for administrative users can be managed centrally. In addition, global changes can be made quickly and consistently under Windows, Linux and UNIX.

5.5 Shared Account Password Management (SAPM)

When implementing PAM projects, PATECCO puts great emphasis on the protection of the assets of the respective organization. Shared accounts ought to be prevented conceptually, because the containment of data protection violations is most effective if the attack surface can be reduced.

The aim is therefore to reduce the number of privileged accounts as far as possible towards zero and to use SAPM only for emergency login scenarios such as "Break Glass". This applies to legacy and emergency scenarios in which privilege elevation cannot be reached sensibly and in which direct logon as administrator (for example, root) must be allowed in exceptional cases.

5.6 Application to Application Password Management (AAPM)

A key design deficiency in programs that require automated access to critical systems (such as provisioning systems or other programs that use service accounts) is the use of hard-coded credentials in application code, scripts, and other configuration files. As described in section 4.2, AAPM tools provide a workaround by providing a mechanism (typically APIs) to make credentials securely available on demand by accessing a secure password vault.

PATECCO supports during the execution of a PAM project in implementing AAPM as an extension of the SAPM tools. This helps in managing accounts used by applications or systems to communicate with other applications or systems (such as databases, web services etc.).

5.7 Summary of Patecco Services for PAM implementation

PATECCO acts as a vendor neutral provider of value-added services and implements PAM solutions deploying products of market-leading PAM vendors, including, but not limited to Thycotic, One Identity, CyberArk and IBM. Apart from that, PATECCO has established partnerships with Microsoft, IBM (implementing Thycotic solutions) and One Identity.

PAM is used as an information security and governance tool to support companies in complying with legal and regulatory compliance regulations. It also helps to prevent internal data misuse through the use of privileged accounts. In case of undesirable behavior, PAM can be used to detect and trace this abuse.

By implementing PAM capabilities, privileged users have efficient and secure access to the systems they manage, while organizations can monitor all privileged users for all relevant systems. PATECCO supports in ensuring that audit and compliance requirements are met and can support in implementing privacy policies adherent to regulatory and legal requirements, e.g. EU-GDPR.

6 Recommendations

Privileged Access Management has grown from a merely basic and security discipline of limited scope to an important component in both IAM and enterprise security. Keeping it up to date, from a technological and from an architectural perspective while maintaining an utmost level of protection for an organization and its assets, is an ongoing challenge.

Managing the use of elevated rights and shared accounts is not only - and not even mainly - a technical problem. Technology helps enforce defined policies and controls, but unless companies have a clear plan as to how they can leverage those technologies and enforce that particular plan, Privilege Management Tools are nothing more than fig leaves covering weaknesses in a company's IT security.

Keeping up with the modern cybersecurity and compliance challenges without breaking the bank requires careful planning. We recommend considering the following:

- **Continuously adapt PAM to your changing IT and business**
  A PAM system can only be as effective as its integration into a continuously evolving IT landscape. Privileged accounts and the risks associated with them evolve along with ever-changing systems. They thus reflect conceptual changes, such as the ubiquitous digitization and the cloud revolution, as well as every hype and trend (think: DevOps, AI, IoT). Continuous adaptation to continually changing systems, their criticalities and administrative peculiarities is indispensable for maintaining the security level.

- **Integrate PAM and Access Governance**
  The integration of Access Governance and Privilege Management at the IAM architectural level enables the definition and deployment of a wide range of governance and administrative processes. It bridges existing governance silos, which are typically manifested by individually maintained repositories (Access Governance access warehouse and the Privilege management repositories of privileged accounts).
  There are use cases where an efficient integration can be achieved by assigning privileged accounts as additional, secondary accounts to IAM-managed identities and by provisioning those accounts into the PAM system and/or the actual target system. Well-executed user lifecycle processes in IAM will make sure that no longer needed privileged access will be deprovisioned.

- **Go beyond the traditional administrator**
  There are primarily two types of privileged users:
  Privileged IT Users – those who have access to IT infrastructure supporting the business. Such access is generally granted to IT administrators through administrative roles using system accounts, software accounts or operational accounts.
  Privileged Business Users - those who have access to sensitive data and information assets such as HR records, payroll details, financial information, company's intellectual property, etc. This type of access is typically assigned to the application users through business roles using the application accounts.

- **Go beyond on-premises**
  Hybrid IT is becoming the new normal and this needs to be reflected in a PAM strategy. Administrative technical and privileged business users in AWS, Azure, Salesforce.com, Workday, Office 365, SAP, SAP HANA, and a vast amount of further cloud services between IaaS, PaaS, SaaS, Docker-platforms and server-less architectures need to be included in an overall hybrid security approach.

- **Integrate PAM into your IT Security, your Incident Management and your SOC**
  Properly designed and executed Privilege Access Management processes are a rich source of security related information. This subsequently makes PAM a data source for various enterprise security infrastructure systems. Correlation of information about Malware outbreaks or targeted network attacks thus can result in alerts to be sent to the Security Operations Center (SOC) and appropriate measures to be taken on an enterprise level.

- **Training and Awareness**
  With the continuous fluctuation of personnel, with changing infrastructures and mostly simply in the course of time, up-to-date knowledge in organizations, especially about security systems, their use and necessity are lost. The importance of training and creating awareness cannot be overestimated. Give your administrators and privileged business users the skills for managing and using PAM they need.

Privileged Access Management has been and will be an essential set of controls for protecting the proverbial "keys to your kingdom". Proper planning and continuous enhancement, strong enterprise policies, adequate processes, well-chosen technologies, extensive integration are key success factors. The same holds true for a well-executed requirements analysis, well-planned implementation, well-defined roll-out processes and an overall well-executed PAM project.

Benefitting from an experienced project partner of the likes of PATECCO can often be beneficial. Bridging the gaps between specific requirements technical and organizational challenges, through technology, compliance, security, and vendor and product experience has often proven to be an important enabler for successful PAM deployments.

7 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, 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 Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com