PATECCO
dynamic identity systems.

Since 2009. High Expertise in Identity and Access Management Competence

January 2022

„Digital workspace compliance through Managed Services for Privileged Access Management to effectively prevent insider threats and data loss"

WHITEPAPER

- PATECCO Company overview and services
- PAM Capabilities and functionalities
- PATECCO Best Practices for implementing Privileged Access Management solutions
- Customer Success Stories

Table of Contents

1.PATECCO Overview

PATECCO is a German company specializing in development, implementation and support of Identity & Access Management solutions. Based on 20 years' experience within IAM, high qualification and professional attitude, the company provides value-added Managed services with fixed prices to customers from different industries such as banking, insurance, chemistry, pharma, utility and education.

PATECCO's long-term partnership with Microsoft and IBM supports the success in a number of international consulting projects. Furthermore, our team of proficient IT consultants provide the best practices in delivering comprehensive solutions based on latest technologies:

- Cloud Access Control
- Privileged Access Management
- Identity Governance and Intelligence
- Role Based Access Control
- Recertification
- Security Information Event Management

The main benefits that PATECCO ensures are related to several key points:

- **Reliability and Security:** we develop reliable IAM solutions tailored to your business needs, which ensure high protection of sensitive data and proper management of identities. We also help organizations meet compliance requirements.
- **Flexibility:** we offer 3 levels of support for managed services - Remote, Onsite Support for Business-Critical Issues, and Onsite on Demand.
- **Global capability:** our solutions support clients of all sizes and industries around the world and support them to be successful in the digital transformation by replacing old IAM paradigms through innovative models.
- **Fixed-price projects:** We offer fixed-price projects which are based on defined scope.
- **24/7 remote management and monitoring:** Our experts are not only available all the time, but they also respond quickly to your needs and problems. PATECCO team is also available for onsite support which is a huge benefit to making sure you have the best service delivery.

2. Solutions & Services

IAM solutions must be an integral part of any enterprise security system. Their central management capabilities can help in improving security while decreasing the cost and complexity of protecting user access and credentials. In addition to providing access to employees, organizations also need to work, collaborate, and connect with contractors, vendors and partners, each with their own set of access requirements and restrictions. Furthermore, data and applications spread across cloud, on-premises and hybrid infrastructures are being accessed by a variety of devices including tablets, smartphones, and laptops.

The Solutions & Services which PATECCO provides are IAM Consulting, Managed Services, PAM, SIEM, Cloud Access Control, IGI, RBAC and Recertification.

O IAM Consulting

In each phase of our consulting projects the right resource is assigned to specific activities. Our team of architects, consultants and developers are able to drive your project successfully. In our practice, we deliver projects on our own or provide resources for your project staffing.

Our IAM Consulting includes:

- User provisioning and synchronisation as a single solution
- Managing and maintaining Directory Services domain migrations
- End-to-end implementing and managing of FIM/MIM solutions
- Full management of identities, privileged access management and integration with any Cloud platform along with Identity Governance and Intelligence (IGI)
- Consulting and Deployment of QRadar

As regards to Business analysis, we are working very close together with the top business analyst firms and well-known security auditors. And this background supports us during our consulting projects, where we perform activities, such as:

- Focus on Governance, Risk & Compliance
- Analysis of core business processes in regards to regulatory requirements (SOX, BAFIN, BASEL II, HIPAA, FDA, etc.)
- Validating and developing company compliance and governance policies
- Analysis of core business processes in respect to vulnerability, security and risk
- Introducing and implementing industry standards

2. Digital workspace compliance through Managed Services

Nowadays the technology is moving at a faster pace than ever. Whilst advances in technology present a number of opportunities, they also present businesses with challenges they must manage effectively in order to remain successful and profitable. Many businesses have users with multiple computer models and operating systems, so it can be difficult to manage costs and keep people connected and productive. This is where Managed services can help. They include any information technology service and support handled by an outside firm through cloud-based software.

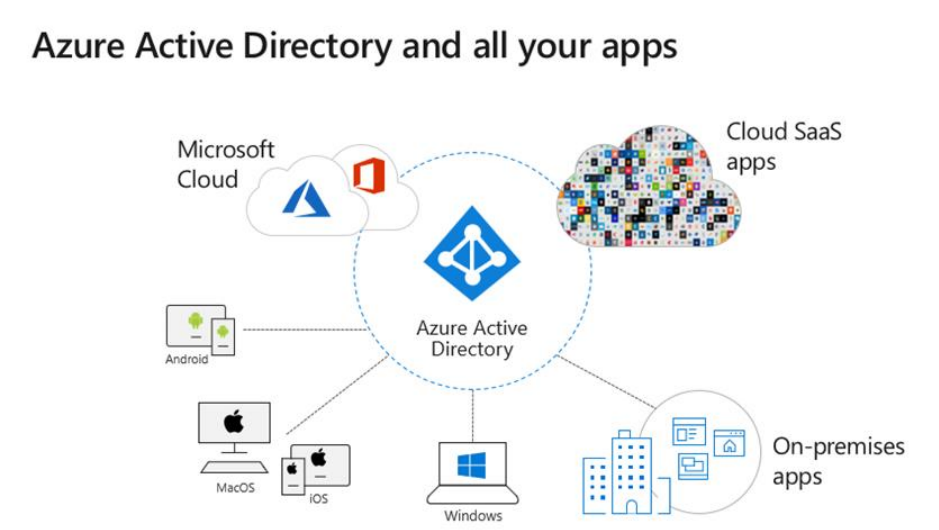
These information technology solutions provide remote monitoring of your systems, along with proactive support, and timely managing, updating and resolving issues in real time related to selected IT systems and functions on your behalf.

As a managed service provider, PATECCO ensures a cost-effective alternative to manage the monitoring, detecting, investigating, responding to cyber threats. PATECCO Managed services ensure the visibility for better protection of your sensitive data and critical infrastructure, and the incident response solutions provide rapid response and recovery to cyber threats.

Our team of professionals is proactive and manages your IAM services available 24/7 for your peace of mind. And as your managed service provider, PATECCO offers a single point of contact, convenience and flexibility for all of your IT needs.

3.Cloud Access Control

When talking about Cloud Access Control, PATECCO offers a clear migration path from on-premise Active Directory to Azure AD Domain Services providing benefits such as flexibility, security, efficiency, scalability and compliance.



O Cloud Access Control Benefits

Flexibility: provides an access to every location and every employee can be managed from one platform. And the central management and monitoring of access permissions provides a high level of flexibility for a business.

Security: refers to the ability of the cloud system to detect and trace any anomalies that occur in the system and act accordingly.

Efficiency: the automation capabilities of cloud access control maximizes the end-user efficiency, protect company data, and transition to a digital workspace.

Scalability: Thanks to that feature your system can react and adapt to changing demands. In case your company grows, you will be able to seamlessly add resources without losing quality of service or interruptions.

Compliance: From our experience, we know that some industries, like financial institutions and ecommerce, have more industry and governmental regulations

than others. A robust cloud solution can provide an enhanced infrastructure that supports regulatory compliance and protects consumers' personal and financial data.

4. Identity Governance and Intelligence

We know that Identity Governance and Administration (IGA) provides the identity foundation that powers today's most important security initiatives, including Zero Trust, Digital Transformation, and Cyber Resilience. In the area of IGI PATECCO performs activities such as:

Access certification: IGI enables the business to run access certification campaigns to reconfirm users access needs with a customizable, self-service user dashboard. IGI uses a unique business activity-based approach to model separation of duty violations rather than relying on unmanageable role-to-role comparison.

End-to-end user lifecycle management: where IGI automates the identity lifecycle process and reduces the need for manual labour.

IGI helps you identify areas of risk and access optimization through powerful identity analytics, providing priceless visual insights on risky users and behaviors. We also perform integration with privileged access management products and integration with QRadar UBA (User Behaviour Analytics) for insider threat management

O IGI Benefits

Here we will summarize the major benefits of IGI which refer to improved productivity of the daily work, ensured compliance, reduced costs, decreased vulnerabilities and most of all - increased security and enhanced confidentiality which means that only the authorized users have an access to the necessary data.

5. Role-Based Access Control

In organizations, like yours, that have major divisions, creating a role-based access control system is essential in mitigating data loss and the best solution for enhanced security. With role-based security, you can achieve both optimal data protection and user productivity by granting varying levels of permissions to users based on their role.

There is another important thing in RBAC – that a distinction should be made between manually assigned roles or automatically assigned roles based on HR data such as organization or position / location, etc. These cannot be ordered and are automatically assigned or withdrawn when the change is made.

O RBAC Benefits

A great advantage of RBAC is the ability of giving you granular visibility, which is necessary to securely support your mobility in today's digital environment.

Another benefit of RBAC refers to maximized operational performance allowing your company to streamline and automate many transactions and business processes.

6. Recertification

By recertification we continually auditing users' permissions to make sure they have access only to what they need. And the tasks we perform in our projects are related to:

- Recertification of employee's authorizations for roles / groups / responsibilities (owner)

- We also make Recertification of the authorization objects themselves. So whether the configuration of the role still fits (especially group affiliations, descriptions)

- Recertification can either take place after a defined period (annually / semi-annually) or at a fixed point in time.

- Transfer processes of a user always include the recertification of authorizations or even the withdrawal

3. Why PAM should be your highest cyber security priority?

Cyber security is a hot topic for every enterprise in today's hyper connected world. With the fast-growing technologies like cloud, mobile and virtualization, the security boundaries are a little bit blurred and not each organization protects its valuable and sensitive information properly. As a result, cyber-attacks and data leakages occur more often and that's why they are no surprise in the Information Security field. With the increasing sophistication of attacks on organizations of all sizes, the question is not whether the company will suffer a cyber-attack, but when that attack will take place, and what its consequences will be.

Controlling privileged actions in a company's infrastructure enables IT systems to be protected from any attempt to perform malicious actions such as theft or improper modifications to the environment – both inside and outside the company. In this context, a Privileged Access Management (PAM) solution can be considered as an important tool to speed up the deployment of a cybersecurity infrastructure.

When it comes to controlling access to a company's cloud workloads, big data projects and network devices, our experience shows that most enterprises are not doing enough to address modern security concerns. Some of the worst data breaches in recent times were a result from the abuse of privileged accounts and the impersonation of privileged user identities. That is why over the past few years, PAM has emerged as one of the most crucial IAM technologies for preventing security breaches and credential thefts.

There are also another main reasons why Privileged Access Management (PAM) is essential for all businesses and why it should be their highest cyber security priority:

- **PAM ensures high level of security for privileged credentials**

PAM has drastically changed the way enterprises protect access to critical systems. Using credential vaults and other session control tools, PAM has allowed managers to maintain privileged identities while significantly decreasing the risk of their compromise. By centralizing privileged credentials in one place, PAM systems can ensure a high level of security for them, control who is accessing them, log all accesses and monitor for any suspicious activity.

- **PAM enhances compliance**

Nowadays a large number of corporations have to comply with industry and government regulations and that leads to more challenges. For better compliance a PAM solution enables you to get in control of managing and securing privileged accounts to meet the needs of the access control requirement for a good number of the regulations, fast-tracking your way to being compliant.

- **PAM enables fast recovery from cyber-attacks**

In case of a cyber-attack your Privileged Access Management solution gives you the opportunity to quickly audit privileged accounts that have been used recently, to discover whether any passwords have been changed, and to determine which applications have been executed.

Moreover, PAM can help compare a baseline to before and after the incident, so you can quickly determine which privileged accounts might be malicious and audit the life cycle. This is a good way to ensure recovery and maintaining the integrity of your privileged accounts.

- **PAM provides a high return on investment (ROI)**

One of the main reasons that Privileged Access Management should be a top priority for organizations in 2022 is that it could save them time and money. On one hand, most cyber security solutions only reduce risk, and a lot of enterprises spend valuable budget on security solutions that actually add no additional business value. On the other hand, the right PAM solution makes employees more productive by giving them access to systems and applications faster and more securely.

4. PATECCO PAM capabilities

In its practice 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 IBM, Thycotic, One Identity and CyberArk. Apart from that, PATECCO has established a partnership with Microsoft.

PATECCO develops, implements, and manages PAM 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. 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.

Furthermore, to control privileged accounts effectively and efficiently, PATECCO requires a combination of adaptive access management capabilities. They are directly associated with the areas **"Auditability, Administration, Analysis",** "Authentication" and "Authorization".

- **Auditability, Administration, Analysis:** When we observe privileged account activity, we always assure our customers, that the combination of auditing, administration, and analytics in one software tool can reduce the privileged account risk. Auditing of privileged accounts gives them metrics that provide executives with vital information to make more informed decisions as well as demonstrate compliance with policies and regulations. Further implemented PAM software by PATECCO simplifies the annual audit process by external auditors and shorten the duration significantly as our customers are passing through future audits faster with less costs.

- **Authentication:** It is mostly related to multi-factor authentication. It authenticates a user and grants access only after presenting two or more pieces of proof (or factors) to an authentication provider. MFA helps protect against password compromise by requiring at least one more form of identification.

And the third one is:

- **Authorisation:** Is used based on company policies which PATECCO can help to develop to give the user permission to access a specific resource or function depending on his role. In secure environments, authorization must always follow authentication. Users should first prove that their identities are genuine before an organization's administrators grant them access to the requested resources.

5. Core functionalities of PAM tools

Privileged Access Management tools are designed to significantly enhance the protection of an organization's digital assets by preventing misuse of privileged access. As I mentioned before, 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.

The proper management of privileged access helps organizations prevent devastating data breaches and comply with regulatory requirements. But at the same time, it can be difficult for security teams that are understaffed and struggling to maintain access information across complex IT infrastructures. By providing comprehensive and clear visibility into privileged accounts, implementing least privilege, investing in the right solutions, and monitoring activity, you can be able to prevent privileged accounts from being abused and effectively tackle security risks both inside and outside your organization.

Core functionalities of PAM tools are:

- **Credential vaulting**

It is related to the technology and processes for the secure, audited storage of and access to passwords and similar cryptographic key material.

- **Password rotation**

It is the reduction of the lifespan of passwords by changing it frequently to reduce the risk of compromise, especially for critical accounts.

More advanced functionalities such as privileged user analytics, risk-based session monitoring and advanced threat protection are becoming the new norm. Here we can also add that with the attack surface expanding and the number and sophistication of attacks increasing every year, is required an integrated and more comprehensive PAM solution, that can automatically detect unusual behaviour and initiate automated mitigations.

Customer Success Stories

UNIPER

PATECCO´s first customer with a Managed-Service-Contract for Privileged-Access-Management is UNIPER SE.

Uniper SE operates as an international energy company. The company owns and manages a portfolio of power plants located across Europe and Russia, as well as focuses on commodity trading business, such as power, emission certificates, natural gas, liquefied natural gas, coal, and freight. Uniper also operates power and gas storage facilities.

Uniper SE has implemented a Privileged Access Management System in a very short time, with the support of PATECCO. In addition, Uniper SE used a service contract to operate this solution at its headquarters in Düsseldorf, Germany, as well as its power plants across Europe with PATECCO Managed-Service.

Why Uniper SE chose PATECCO?

- PATECCO was not only able to implement the new PAM-Solution, but was also able to guarantee regular operation both in the head office and in the power plants.
- The managed service contract not only includes monitoring, but also the possibility to make use of on-call service for specific requirements.
- Working in accordance with DIN ISO 27001 is a mandatory requirement.
- A complete integration of the service processes in ServiceNow was specially developed by PATECCO and adapted to the customer's requirements.
- The whole process is monitored and controlled by monthly meetings and management reports.

Customer Success Stories

VM GRUPPE

The company is as part of WM Gruppe and is responsible for issuing the German Securities Identification Number (WKN) and, as the National Numbering Agency it is also responsible for issuing the International Security Identification Number (ISIN) of German issuers, the CFI (Classification of Financial Instruments - ISO 10962) and the FISN (Financial Instrument Short Name - ISO 18774) for all types of financial instruments. Since November 2012, WM Datenservice has also been accredited as an issuing authority for the Legal Entity Identifier.

WM Gruppe has implemented a Privileged Access Management System and an Identity Access Management system with the support of PATECCO.

Why WM Gruppe chose PATECCO?

- One of the reasons is that PATECCO was able to implement both a PAM and an IAM solution which enables the customer to get the full Identity Management package from one supplier.
- Working in accordance with DIN ISO 27001 is a mandatory requirement.
- PATECCO developed the integration of the IAM IT Shop to the USU ITSM (IT Service management) and was also adapted to the customer's requirements.
- The project had a fixed monthly budget.

72 Ringstrasse; 44627 Herne, Germany,

+49 (0) 23 23 987 97 96; info@patecco.com www.patecco.com