PATECCO
dynamic identity systems.

March 2020

PATECCO Identity and Access Management Solutions in Financial Service Industry

WHITEPAPER

- Identity and Access Management
- Role-Based Access Control
- Identity Governance and Intelligence
- Privileged Access Management

Table of Contents

1.Introduction

The modern financial enterprise needs to keep its data protection on the same high level as it keeps its core business, as well. The amount of data financial firms capture keeps growing, and so does the need to share it safely with customers, partners, vendors, and employees.

Financial institutions must be sure that users are who they say they are, and that they only access the data their privilege status allow. Password policies are only able to restrict who can enter a system, but once being inside, users' activities should be controlled by a robust identity and access management solution.

No matter it is deployed in the cloud, on-premise, or in a hybrid environment, PATECCO IAM solutions are seamless, secure, and compliant. That means that they help financial organizations do business safely in the connected world.

The problems that a bank can encounter are the same that may be faced by an insurance company, a group of hospital or a professional industry body. But these organizations can now implement centralized, shared solutions, accessible by all their various branches, subsidiaries and partners. Moreover, they still need to be better provided with security, user-friendliness and traceability when it comes to accessing services.

1.1 Significantly Increased Security and Compliance with Regulatory Provisions

The level of security and quality of the IT processes and systems employed at a financial service provider determine the level of IT risk associated with its daily business. You can reduce the security risk with the help of the Identity & Access Management Solutions. The functions as well as the IT access needs of people are always subject to changes. Whether employees, partners or contractors – access authorizations should be adapted to new structures and needs on an ongoing basis. There are many factors and situations that should be considered in the context of data security, including employee relocations, terminations or the speed of setting up new accounts and authorizations. The IAM services provided by PATECCO boost the efficiency and economy of IT-driven workflows and thus act as a strong enabler of digital transformation in the financial sector.

1.2 Protect your sensitive information, data and systems from unauthorized access

The growing threat of data misuse and theft, along with the current complex legal regulations (HIPAA, GLBA, SOX) make IAM systems a mandatory tool for businesses from the financial sector. PATECCO IAM Services protect the business-critical information, data and applications of financial service companies from unauthorised access. At the same time, the IAM tools facilitate the digital

transformation of companies and provide powerful functions based on best-practice processes. They are all designed to improve data security, reduce risk relating to data access, and introduce efficient audit-compliant processes that ensure compliance with all legal regulations.

As a result of the regulations, the active enforcement of "Segregation of Duties" became much more important. Segregation of Duties (SoD) refers to the discipline that enforces operational checks and balances. SoD controls the execution of various processes, preventing potentially compromising positions for employees. It often separates a process and its verification or enforcement. These controls may distribute various aspects of a process amongst employees or business units. They may require multiple authorizations. A government's separation of those who pass, verify, and enforce laws serves as an example.

2.The Progress and Advantages of IAM in Banking

Financial services organizations are investing significant resources in cloud-based technologies, including infrastructure, platform and software as a service. These allow for rapid scaling, moving operational burden from the organization to expert third parties, and can add substantial value and competitive advantage.

Many organizations struggle to support IAM and privileged access management (PAM) in these environments in a way that both adds business value and mitigates the aforementioned risks. This means that IAM organizations must balance business desires around factors like streamlined and smooth authentication experiences with compliance requirements indicating when MFA or risk-based authentication is mandated (e.g., in order to access any personally identifiable information, for all privileged activities, etc.). Similarly, administrator-level users with high-risk levels of access to sensitive data may need to perform their duties with advanced PAM controls like session recording, even if it slightly impacts user experience.

2.1 Ensuring Security and High Business Value With Role-Based Access Control

In the era of digital transformation the tight privacy laws have imposed new levels of confidentiality on health care, insurance companies and financial institutions. As the number of their electronic systems increases along with the number of interfaces, identity management has become a critical component in ensuring information security and access control. Access control plays an essential role in safeguarding both physical security and electronic information security. Role-based access control could be simply explained as the security process of assigning specific rules or policies to individual users, or groups of users, that are connecting to your network. It simplifies the process in assigning user's access based on their job function.

It has become a critical component in ensuring information security and access control. Access control plays an essential role in safeguarding both physical security and electronic information security. Role-based access control could be simply explained as the security process of assigning specific rules or policies to individual users, or groups of users, that are connecting to your network. It simplifies the process in assigning user's access based on their job function.

Developing and using a role-based access control system in conjunction with an identity management solution makes it possible for organizations to ensure that accounts for new employees are always created with proper access rights. That means that there is a control defining which users have access to resources based on the role of the user. Access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role. For example, if a RBAC system is used in a hospital, each person

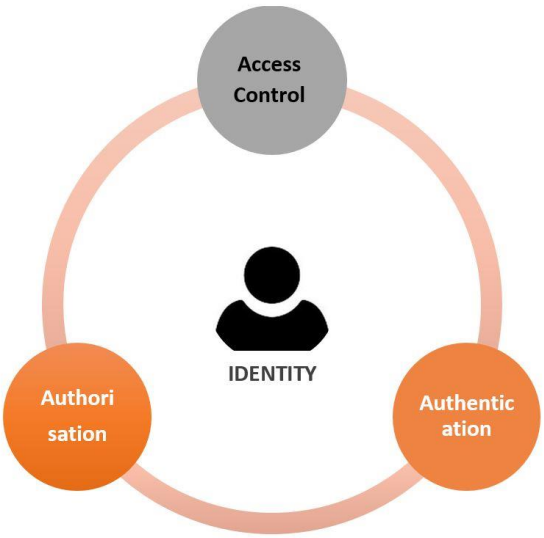
that is allowed access to the hospital's network has a predefined role (doctor, nurse, lab technician, administrator, etc.). If someone is defined as possessing

the role of doctor, than that user can access only resources on the network that the role of doctor has been allowed access to.

2.2 Four steps for providing data security

There are four steps which are of a great importance for providing proper data security.

- The first phase is to ensure that new employee access and accounts are created properly when the employee is on boarded.
- Second phase refers to giving those access rights remaining accurate and up-to-date during each of the company's employee's tenures.
- The third, and most essential step in this process, is revocation of access rights when individual employees leave the organization.
- The fourth step is performing Information audits. The sooner you get used to them, the better. They are required to successfully manage the information and the access of rights. Our advice is to periodically review your roles, the employees assigned to them, and the access permitted for each. Once an audit of access rights is performed, it can be compared against the baseline template for each employee role initially established. If needed, the managers and systems owners could make for verification or revocation of the rights.



2.3 What are the benefits of RBAC?

Ideally, the RBAC system is clearly defined and agile, making the addition of new applications, roles and employees as efficient as possible. One of the greatest advantages 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. Thus, companies could streamline and automate many transactions and business

processes and provide users with the resources to perform their jobs better, faster and with greater personal responsibility. With RBAC system in place, organizations are better positioned to meet their own statutory and regulatory requirements for privacy and confidentiality, which is crucial for health care organizations and financial institutions.

Organizations should implement necessary security measures to provide that access to data, groups and applications are right for an employee during their tenure. They also should bear in mind that quite critical is the revocation of all account access when they depart. Failure to respond these criteria can lead to data theft and costly access to external applications. Furthermore, working without access restrictions could lead your enterprise to the following problems:

- Improper or fraudulent use of a company asset
- Insider trading
- Employees could fraudulently route funds to themselves
- Employees editing their own work may not catch a mistake or may be able to abuse noncompliant access
- Hiring staff may offer a friend a position or inflated compensation over other applicants
- An employee could create and cover-up an order discrepancy to take goods for themselves

3. What Does Identity Governance and Intelligence Do to Protect Your Business

In today's interconnected marketplace, organizations are challenged more than ever to address regulatory controls and compliance mandates. They also must control access to key resources to protect their data and intellectual properties, being at the same time unique and innovative. For that purpose, it is critical to create effective methodologies, tools, and workflows for managing access and proper identity administration across the enterprise.

And talking about a solution for securing the company sensitive information and network, comes the question concerning all: How do you manage all of your enterprises' identities? Do you stay in compliance with regulatory mandates and do you adhere to high standards of privacy and protection?

This is where Identity Governance and Intelligence solutions come in. They are designed to help enterprise IT departments automate their identity workflows, manage manage identities and application access and to stay in compliance with thorough reporting. Besides, Identity governance incorporates measurable access risk controls that helps to set policies and to better drive activities such as access review, privilege management and the management of separation of duties. It

provides an integrated, streamlined approach for managing user roles, access policies and risk, ensuring that appropriate levels of access are applied and enforced across enterprise and cloud applications. The solution automates the administration of user access privileges across an organization's resources, throughout the entire identity management lifecycle.

3.1 Use of IGI

Within the enterprise and between enterprises, the users require access to the systems and data necessary to perform their jobs. Most businesses outsource services and work directly with partners and suppliers, that's why they are faced with the additional problem of giving access to people outside of the organization. No matter where the employee is located and whatever organization they are part of, their access needs to be managed and precisely controlled to lower the risk of fraud and ensure compliance. Governing the way this access is assigned, managed and monitored, is essential activity for the security of the business.

Organizations are obliged to comply with the increasing range of laws and regulations. Proving compliance requires an audit to confirm that the access to this data is properly managed. When there is a lack of good identity governance, these audits can be time consuming and expensive.

The use of mobile phones, tablets and other devices by employees and partners to access company's systems and data creates a new set of risks. Identity and access governance can help to manage these access related risks. Auditing access rights and controlling the different kinds of duties can be very difficult without the appropriate identity governance tools. These complexities appear when a person performs more than one role.

3.2 PATECCO IGI Capabilities

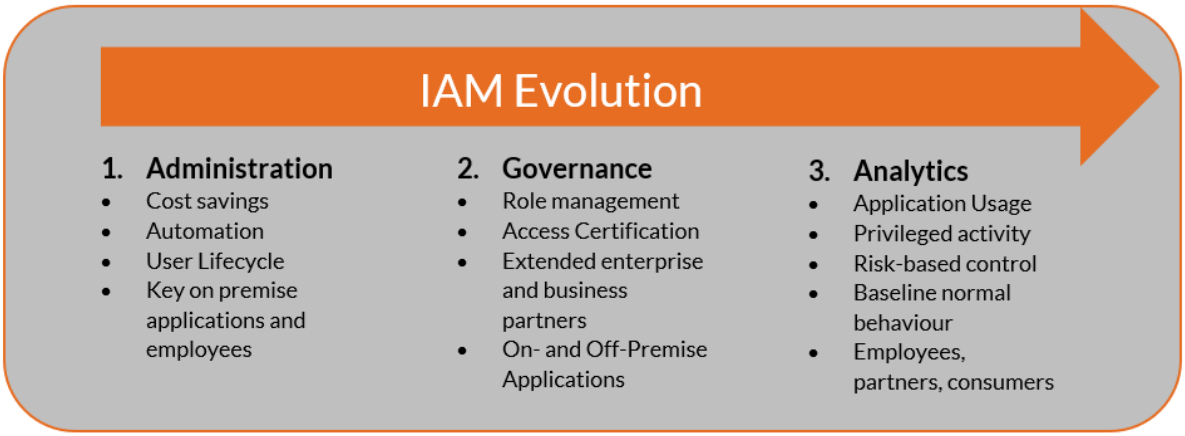
To answer the question – "Who should have access to which resources, when they should have that access, and who decides?", PATECCO provides IGI tools that deliver user administration, privileged account management, and identity intelligence. Its Identity Governance and Administration Services provide the tools, experience, and capabilities to support these initiatives.

PATECCO Identity Governance and Intelligence capabilities can help you to enable automated workflows and streamline existing processes. They also deploy automated access provisioning, identify and manage roles and segregation of duties to balance information security and business knowledge to avoid complexity and security risks. The IAM Company addresses audit reviews and compliance concerns, and ensures that proper protections and controls are in place to remove as much risk as possible.

Identity governance is important for organizations to ensure the security of their IT systems and data, as well as compliance with laws and regulations. Identity governance enables business compliance in consistent and effective manner that adds value, reduces costs and improves security. It ensures that the users have their access rights assigned, minimizes the opportunities for fraud and data leakage by ensuring that data and applications can only be accessed by authorized admins.

3.3 Identity Governance and Intelligence: Benefits

- Improved productivity of managers by simplifying identity and access certification processes.
- Increased general level of security, reduced costs of managing users and their identities, attributes and credentials.
- Ensured compliance in consistent, efficient and effective manner.
- Reduced vulnerabilities and limited risk of data breaches or loss of customer and employee information.
- Enhanced confidentiality - data can be accessed only by authorized individuals.



4.Privileged Access Management

Ensuring and maintaining the security of banking data is a constant concern for the financial sector. Highly wanted personal data and the potential payout it represents to cybercriminals, make the financial sector a prime target. Given the actual number of service providers, involved in each step of a banking transaction, and the processes, which are required to guarantee the security of banking data, are quite complicated.

The new security challenges that come with the digital transformation (think applications, online payment, mobile access, and cloud-hosted services) requires banks and other finance firms to take care of the security and always to demonstrate due diligence. They have to implement innovative solutions that can guarantee the confidentiality, integrity, and traceability of their clients' personal data. To respond these needs, most finance companies rely on the capabilities of Privileged Account Management Solution.

4.1 Eight of the Most Important Features of Privileged Account Management Solution

Privileged access management (PAM) tools are an essential part of any comprehensive cyber security strategy. They are also important element of secure remote user and remote server environments. Protecting privileged accounts ensures your credentials and data are not exposed to potential threats and helps prevent breaches. As a domain within Identity and Access Management, PAM solutions can provide a lot of benefits to your business rather than simply guarding passwords. They allow organizations to effectively protect, monitor, and manage privileged account access to include their life cycle management, authentication, authorization, auditing, and access controls.

To ensure secure working environment, your organization should implement a strong Privileged Account Management (PAM) solution, which allows you to control and restrict access to privileged accounts within an existing Active Directory environment. The fact that there are a lot of PAM products available could make you feel confused in your choice. To help you chose the right one and move forward, here we present 8 critical and mandatory features to look for in a PAM solution.

1. Privileged Session Management

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. The capability to monitor and record privileged sessions provides security experts with all the needed information for auditing privileged activity and investigating cybersecurity incidents.

The challenge here is to associate each recorded session with a particular user. In many companies, employees use shared accounts for accessing various systems and applications. If they use the same credentials, sessions initiated by different users will be associated with the same shared account.

2. Privileged User Behaviour Analytics (PUBA):

PUBA uses data analytic techniques or machine learning techniques to detect threats based on anomalous behaviour against established behavioural profiles of administrative users as well as user groups and administrator.

The anomalous behaviour might not be malicious, but at least you are aware of it, you are able to investigate further. PUBA helps IT and Security administrators to rapidly discover breaches before they occur, analyse how your privileged accounts are distributed and research how they are accessed throughout your organization. This adds an additional level of security to your defence strategy.

3. 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.

4. 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.

5. Privileged password management

When having a privileged password management feature, your PAM solution allows you to automate and control the whole process of giving access and passwords to privileged accounts. These critical and sensitive credentials are given only in case the previously established policy is observed and when all required approvals are met. Privileged access management tool keeps track of all activity on privileged accounts and ensures that passwords are changed immediately after return.

6. Role-Based Security

Another necessary feature you need is the ability to establish role-based security for groups of users who demand the same access level. Role-based security helps you overview who has access to what, and it also lets you effectively track and monitor all changes. For more information about RBAC, read here.

7. Auditing and reporting

PAM tools collect big amounts of data: activity logs, event logs, session records, and so on. But it really doesn't matter how many useful data your PAM solution gathers if you cannot create a comprehensive report out of it. So what you need is to be able to form different types of reports according to your specific needs

and requirements. You also should pay special attention to the type of data and information that can be included in the reports.

The best option is to get a full report about all activities performed under privileged accounts or privileged sessions that were initiated out of the usual working hours.

8. Real-time notifications

Real-time notifications can help you stop the attack earlier when you respond the security incident in time. So, when choosing a privileged access management solution, make sure to check if it has a fine alerting system.

The misuse of privileged access can lead to destructive consequences for your company and to a great opportunity for the attackers to steal valuable and important information. Compliance regulations require secure and properly managed privileged access, which is possible by deploying a quality PAM solution. Here, in this article, we the described the criteria that you should pay attention to when choosing the right PAM solution for your enterprise.

5.Single Sign-On and Multi-Factor Authentication

Single sign-on capabilities ensure that your digital properties and services are easily accessible, no matter they abide on premises or in the cloud. An IAM solution for financial services applications makes it possible for your customers to single sign-on (SSO) just once to access both your and your partner services. It also supports a unified customer profile to ensure your customers' experience continues across channels once they're logged in. IAM enables you to have improved customer experiences from login through logout by allowing each of your digital properties to access a single view of the customer's preferences, privacy consents and other profile data.

When it comes to IAM, one of the easiest security measures an organization can adopt is the addition of Multi-Factor Authentication (MFA). MFA requires the user to enter a pin code, respond to a push notification, or complete another measure following the successful entry of username and password credentials. Without completing the MFA process, the user is not able to log in or access IT resources or data. MFA greatly assists security measures as it provides an extra layer without being a burden on the end-user.

People already use MFA processes to regularly prove their identities outside of IT scenarios. For example, an ATM card requires a personal identification number (PIN). Authentication only occurs when both the card and PIN are used in conjunction. For IT resources, the use of security questions would count as a less-sophisticated MFA policy. Nowadays, MFA can be enforced via One-Time Password (OTP) clients on a mobile phone, push or SMS notifications, or physical security tokens or keys stored on USB or similar devices. The banking and finance industry seem to be ahead of the curve on consumer-facing MFA. For many digital banking platforms and resources, users are already required to complete an MFA step to access their account. The same motivations for protecting individual clients with MFA applies to the employees of any bank or financial service – there’s just an exponential factor of risk.

If you work in the financial services branch, your data protection must be a top priority. You should not only comply with strict regulations around security and privacy, but also to think of a winning IT strategy against cybercriminals, when it comes to protecting your customer and company data.

As experts in identity and access management (IAM), we also know that all these challenges could be solved with a fully integrated and automated identity management solution. You should be aware that Identity Management plays a central role in the digital transformation, including all new business models, applications and ecosystems it supports. Identity Management provides the secure, flexible and adaptive IT infrastructure that every company, government agency or university strives to achieve. It helps to increase customer engagement

through new digital channels, to streamline your business operations and to protect data privacy, and security to keep stable your reputation and finances.