July 2023

Why Identity and Access Management is Critical for Cyber Security in 2023?

WHITEPAPER

- Digital identity management
- Identity Governance and Administration
- Privileged Access Management
- Zero Trust

Identity and Access Management in the era of digitalization

Digitalization is advancing at a massive pace. With the constant development of society and technologies, cybersecurity has also changed drastically in recent years. Especially in times of home office and remote work, cyber security is more important than ever.

Experience shows that small and medium-sized enterprises are not sufficiently protected against digital attacks. However, cyber security (securing and managing external access to critical IT resources) should be a top priority in today's world of increasingly frequent remote access and constant cyber threats.

Identity and Access Management (IAM) is a crucial aspect of cybersecurity because it plays a fundamental role in protecting digital assets, data, and systems from unauthorized access, data breaches, and other security threats. IAM is designed to ensure that only authenticated and authorized individuals can access specific resources, applications, or information within an organization's network.

In PATECCO latest whitepaper, we will provide you a clear understanding why IAM is critical for cyber security in 2023 and how it helps you to keep your enterprise safe and secure.

The series of articles describe the role of Identity and Access Management in cybersecurity which is integral to an organization's overall security posture, adaptability, and resilience against evolving cyber threats. As the threat landscape continues to evolve, IAM will remain a critical component of cybersecurity strategies for organizations aiming to protect their digital assets, data, and sensitive information.

Let’s get started!

Digital identity management - challenges and solutions

Digital identities have become an indispensable part of everyday work and make many things easier. But how can we ensure that a person is really who they say they are? And how can the electronic identities of employees, clients and web portal users be managed securely and efficiently?

Digital identity – what's behind it?

In the private sphere, everyone knows the problem that you have to register on almost every website and fill in a lot of additional information. Although this often seems annoying at first, it is actually necessary. For example, how can you order something online without giving your address, or pay for something without entering a payment source? Since the user does not want to enter the same data over and over again for every action, it is of course possible to save this data in the individual portals, which represents a clear gain in convenience.

On the other hand, this also brings several problems with it. On the one hand, the data in the various portals must be kept up to date. If, for example, a user's address, telephone number or credit card number changes, he or she must also adapt this change in his or her portals, and in the process one or the other portal is often forgotten. On the other hand, every online portal naturally increases the risk that personal data will be "lost" or misused in some way.

Another problem is authentication. How do you prove to the portal that the data you want to use - e.g. to make a purchase - actually belong to you? In the simplest case, this is done by logging in with a user name and password. And that in turn leads to the fact that you have entered this data countless times, which then leads to the well-known "password problem".

- **Digital identities: New working world, new attack vectors**

For many employees as well as companies, hybrid working models as a mixture of office work, mobile work and classic office work have increasingly become the norm and part of the corporate culture, which will probably remain part of the working world even after the pandemic years. This new way of working - flexible and location-independent - has thus also significantly accelerated the cloud adoption of companies: Cloud-based services are now an important part of many business processes and facilitate file sharing and collaboration.

With the increased use of cloud services, however, the number of digital identities is also rising - and these are increasingly becoming the target of cyber attackers. Cyber attacks on digital identities have become one of the biggest threats to businesses.

- **Digital identities within an organisation**

On a smaller scale, in a company or a group of companies, all this can be implemented very well and is already part of the infrastructure in many companies. What falls into this category is the so-called Single-Sign-On (SSO).

Even if there is not yet a definitive solution for this, and certainly not on a global basis, a great deal is already in place. For the overall concept to work, one has to look at several functional blocks. Firstly, there is an identity provider, which is the system that knows the authentication features of the users and also the authorisation. In simplified terms, these are the rights that someone has in a system. In companies, the Active Directory is often used for this purpose, but if you need a more flexible solution with a wider range of functions, there are other systems, as

well. However, the identity provider is only one role, so that users, clients and servers can interact, protocols are also required. The best known and most widely used are OAUTH and SAML.

Probably the most difficult part is the interface between user and system, because on the one hand it should be very secure, since the probability of attack is high, but on the other hand it should also be user-friendly. In the past decades, the simple password concept was used here. Although it has been known for a very long time that this form of authentication is very insecure, it is still the standard, or at least the basic setting. And the reason for this is also simple: it is super easy to implement and understand.

- **Identity management - secure administration of digital identities**

With new mobile devices, the outsourcing of business processes to the cloud and a rapidly increasing number of online services, the demands on data protection and IT security are also growing. On one hand, increasingly comprehensive legal requirements demand an identity and access management system; on the other hand, companies must arm themselves against unauthorised access to sensitive company data, including data leaks and identity theft. Without a central configuration interface provided by an identity and access management system, it is very time-consuming to monitor the currently assigned resources of a user and to be able to analyse and report on them at the push of a button.

- **Targeted assignment of rights**

In companies without a company-wide identity and access management solution, the unintentional accumulation of access rights is not uncommon. During reorganisations or transfers within the company, it is often neglected to delete the old authorisations. Even when employees leave the company, old user accounts are often not or only partially deleted.

An identity and access management solution automatically takes care of the previously used accesses and cleans them up immediately after the departure, so that you are safe from unauthorised access. All this relieves the IT department: it can concentrate on IT operations. Because thanks to central identity management, user self services with automated processes for resetting the access password or for ordering system access for users are also available during the active period.

Conclusion on digital identities and the increasing danger

The attack surface that companies offer hackers is becoming ever larger. Increasing digitalisation and thus also cloud use inevitably leads to a higher number of interactions between people, applications and processes - and thus also to more digital identities, which companies can only secure reliably with a comprehensive identity security approach.

How can Identity Governance and Administration prevent insider threats?

Insider threats are a major and growing concern for organizations, as the human factor is often the most difficult to control and predict when it comes to data security and privacy. With digitization, the amount of digital data is growing exponentially, and with it comes an increase in the number of systems and human interactions with data. More interaction means that data is exposed to more security vulnerabilities.

The potential risks from insider threats are numerous, including financial fraud, data corruption, theft of valuable information and malware installation. These incidents can lead to data breaches that expose sensitive information such as personally identifiable information (PII) or intellectual property (IP) and can result in large fines, while their detection is no easy task for security teams.

What are insider threats in cybersecurity?

Insider threats are cybersecurity risks that originate within the organization itself. They can be caused by users with legitimate access to the organization's assets - including current or former employees, contractors, business partners, third-party vendors, etc.

Insiders can vary significantly in awareness, motivation, intent, and level of access. Traditional security measures such as firewalls or antivirus systems focus on external threats and are not always able to detect threats originating from within the organization. In addition to being invisible to traditional security solutions, attacks from insiders can be more difficult to detect or prevent than attacks from the outside and can go unnoticed for months or years.

Difference between internal and external threats

In many ways, insider threats can do far more damage than external threats. This is because an insider threat potentially has direct access to sensitive data and critical applications, which it can exploit by moving laterally and vertically until it reaches its desired target.

For example, it is easy for cybercriminals to hack an administrator's account to gain access to the root server and database system.

Most companies are also not adequately protected against attacks from the inside, making them much easier to carry out than attacks from the outside. And in many cases, the attacker can carry out his malicious activities undetected. For example, a hacker can trick a user into giving him his credentials, which then allows him to log in as a legitimate user and steal data without being noticed. He could also gain access to a trusted insider, and then lie in wait until he achieves his goal. Without IGA tools, administrators would never notice this because there are no guardrails to guarantee a minimum level of privilege.

Finally, the measures that protect against external threats are largely useless against internal attacks, as they are simply bypassed. Therefore, specialized solutions are needed to effectively combat them.

How IGA can help mitigate insider threats

An IGA tool is a fundamental protection against insider threats. That's because it addresses the core of what makes insider threats dangerous and effective - identity theft. GA provides a streamlined way to manage an organization's identities, including user accounts and access rights. Ensure that employees, contractors and outsourced IT departments can only access network resources designated for them. In addition, access rights can be granted or revoked automatically, depending on the situation. For example, if the system suspects that an account has been compromised, it can revoke all privileges to prevent the account from further penetrating the network. This is also useful for tracking down and deleting orphaned accounts that are easy targets for insider attacks.

IGA tools also have monitoring and analysis capabilities that constantly check user activity. If an irregularity is detected, the account in question can be immediately blocked as a preventative measure. In other words: IGA is like a watchful eye, keeping an eye on the network around the clock.

A robust IGA solution combines user lifecycle management, role-based access control, and automated auditing to reduce the risk of unauthorized data breaches. It also enables organizations to scale and keep up with changing business needs thanks to the following capabilities:

- **Automated User Lifecycle Management:** The Automated User Lifecycle Management feature helps you protect against insider threats by reducing the number of users with access to confidential data. It also mitigates the risk of hackers and security breaches by providing a comprehensive view of user activity across all platforms.
- **Role-Based Access Control:** RBAC limits network access to users according to their role within the company. This best practice reduces the risk of breaches by preventing unnecessary access, such as the ability to view or modify files. Another advantage of RBAC is that it helps limit access to resources, such as applications and data. It also allows companies to define the permissions required for each user and resource easily.
- **Automated Auditing:** It can help you identify suspicious behavior and prevent insider threats. It is also capable of detecting unauthorized access to critical applications. Automated auditing enables you to create traceable, consistent processes and produce reliable and accurate results. These standardized systems and procedures ensure that auditing is conducted the same way each time to detect errors quickly.
- **Compliance Management:** Compliance management software can help you protect against insider threats by limiting access to sensitive information and applications. It also enables you to comply with regulatory requirements, saving your organization money and reputational damage.

How to protect your digital assets with Privileged Access Management?

In the digital environment privileged user accounts provide access to each organisation's most valuable and sensitive assets. Such sensitive assets could be client-confidential information, intellectual property and financial data. Generally, companies keep constant monitoring of regular users and at the same time limit employees' or customers' access to avoid information leaks, misuse and platform changes.

So, without the adequate protection of your privileged accesses, you may receive attacks from external hackers or even from your own employees. For this reason, here, in this article, we explain what PAM is and how it can efficiently protect your digital assets.

Key questions concerning your cyber security

Let's assume that you're one of the many companies that still use spreadsheets and even paper documents to track and managed privileged access. This means that you are not able to have any insight into the real state of security on your most critical systems. And there is a much higher risk of costly and damaging breaches. In this context, to avoid such a critical situation, there are a few questions you must internally consider.

For example:

- ✓ Do you have a clear and enforceable policy for password strength and rotation that is applied to all systems?
- ✓ Do you have a consolidated view of all privileged user accounts, and can you quickly provision and deprovision these?
- ✓ Do you understand which users have access to which digital resources, and can you conveniently and securely elevate privileges where required?
- ✓ Can you review and replay user activities in the event of a suspected breach?

If the answer to any of these questions is "no", you definitely need a modern PAM solution capable of managing privileged access to all systems across your entire network, both on-premises and on the cloud. Through the automation of consistent, repeatable processes, modern solutions make PAM simple, scalable and cost-effective, and empower you to:

- Discover and managed privileged accounts in a highly automated way
- Manage the PAM environment, with user-friendly workflows for obtaining privileged access
- Store passwords and keys in a heavily encrypted vault, and automatically enforce password policies
- Monitor and control privileged access, recording user sessions and maintaining secure audit logs

- Secure and protect the IT landscape by preventing unauthorised use of privileged accounts
- Connect authorised users to systems via session launchers with embedded credentials, keeping the actual passwords hidden.

Role of Privileged Access Management in Protecting Digital Assets

Privileged Access Management is a robust and powerful cyber security solution that keeps most cyber-criminals moving to another target that is not using a PAM solution. Integrating PAM as part of the broader category of Identity and Access Management (IAM) ensures automated control of user provisioning along with best security practices to protect all user identities. PAM security can also be integrated with Security Information and Event Management (SIEM) solutions. This provides a more inclusive picture of security events that involve privileged accounts and gives your IT security staff a better indication of security problems that need to be corrected, or those that require additional analysis.

PAM can also be used to improve insights into vulnerability assessments, IT network inventory scanning, virtual environment security, identity governance, and administration and behavior analytics. By paying special attention to privileged account security you can enhance all your cyber security efforts, helping safeguard your organisation in the most efficient and effective way possible.

- **Endpoint Privilege Management**

Endpoint Privilege Management reduces the vulnerability in your endpoint privileges. Limits and monitors all computing devices and structures. Whether they are computers, servers, as well as IoT and ICS resources. It allows you to elevate the security levels of specific applications, prevents the credential transfer, audits daily access activities, and executes high commands without granting root access.

- **Remote access control**

PAM enables you to reduce the permissions of your vendors and employees without interfering with their work. PAM can send privileged access without sharing your VPN or creating security breaches in the transmission of data packages. It also allows you to designate to administrators the necessary tools to execute processes while closing the entrance to other modules, applications, and commands that are not necessary at that moment.

Besides, the reporting system of PAM software is in charge of documenting the trace of the users in your systems. It records statistics and follows changes, so in this way, you can control the level of SLA and other protocol compliance by third parties and your IT department.

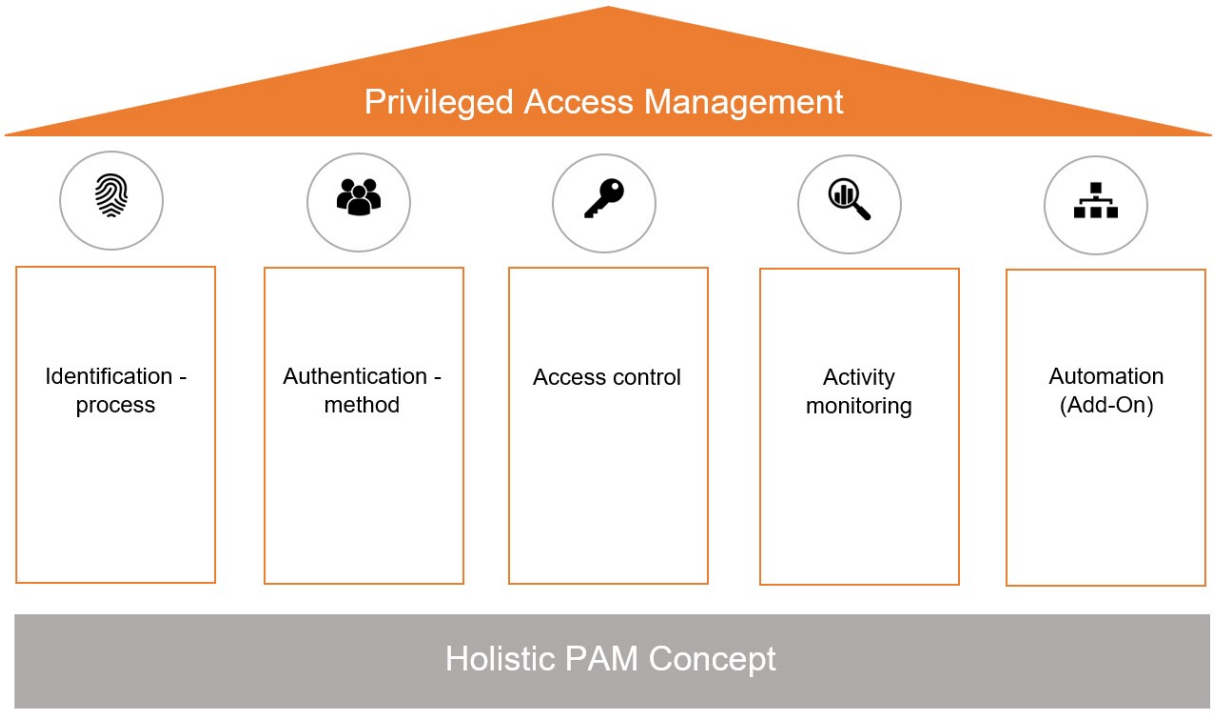
- **Threat management**

PAM software is perfect for vulnerability prioritization. It uses intelligent scanning to identify, analyze, and take action on vulnerabilities across all your digital assets. Whether hosted on-premise, in the cloud, in virtual infrastructures, in mobile devices, or in containers. Moreover, you can compare the performance of systems to industry standards, legal regulations and various security protocols. With this holistic analysis, it is easier to make decisions about privileged access dynamics, consider implementing other technology solutions, eliminate processes and change workflows.

Go ahead for security

Managing privileged access is an essential component of an organization's overall identity governance strategy. With a solid PAM solution, businesses can be confident that they are granting privileged access to those who require it while safeguarding their systems from destructive attacks that could collapse the business and ruin its reputation.

With 20+ years of experience in Identity and access management, PATECCO knows all about data security. We can get you up and running with a best-practice PAM solution based on IBM technology within a matter of days. To get full control of your privileged users and protect your critical digital assets, get in touch with PATECCO today. We are happy to support.



Strengthening cyber resilience with Zero Trust

The exponential growth of cyber threats such as malware and data exfiltration has seen officials at all levels of federal, state, and local government reevaluating their best practices for securing their IT systems and critical infrastructure against malicious actors who threaten their wellbeing.

Add to that, traditional IT security defense are failing, allowing bad actors to get through firewalls and anti-virus products. And, for organizations and agencies with limited resources and capabilities, these attacks represent an especially significant concern, and many are turning to Zero Trust Data Management principles to harden security measures and adopt secure access controls across networks, applications, and devices.

Building Cyber Resilience

A pivotal factor in building cyber resilience and proactively preparing for the next attack starts with ensuring your organization maintains good cyber hygiene. In a nutshell, cyber hygiene is the practice of fundamental security behaviors, amplified through the adoption of supporting processes and technical controls. It's nothing revolutionary — back up your data, patch when you're told to patch, segment your networks, micro-segment your applications and workloads, etc.

One proactive security framework that has gained popularity and more widespread adoption over the last several years is zero trust. A key component of achieving zero trust security is zero-trust segmentation (i.e., microsegmentation). It's designed to stop lateral movement and reduce the attack surface by breaking down the internal infrastructure (think the data center, cloud environment, network, etc.) into smaller segments. In simple terms, think of microsegmentation like a hotel. Just because you're able to get into the hotel doesn't mean you're able to automatically access your room. Because every room has a key, you can only access yours once you're checked in and your access is granted.

Microsegmentation is the critical component of the workload and application pillar of zero trust reference architecture and your zero-trust security strategy; it's designed to stop the spread of cyberattacks and, malware, by isolating workloads and devices across the entire hybrid attack surface. Successfully implementing zero trust takes effort but ensuring your security team has an action plan in place and is taking small steps forward will ultimately better position you and your software supply chain to combat and withstand evolving threats.

Zero Trust Model

As both cyber risks and insider threats to data become too big to ignore, the zero trust model is being adopted as an important component of cyber resilience. The underlying principle is that enterprises cannot enforce less rigorous authentication and authorization protocols for insiders, compared to outsiders. If they do, they could be exposing themselves to a high degree of risk and vulnerability because insiders cannot be trusted any more than outsiders.

The zero trust model focuses on establishing user credentials, motives, and other meta-data such as location, security perimeters, and end points to determine if users can be trusted with data access. It calls for a strong governance and compliance framework to determine user access rights and authorization matrices. Privileged access rights are minimized with multi-factor authentication, identity and access management, and encryption and behavioral analytics.

With the increasing adoption of the cloud and mobile technologies, organizations have realized that information protection needs a different way of thinking. Restricting access to data based on a “never trust, always verify” approach is an effective way of protecting valuable assets.

Three key elements for implementing Zero Trust security

The three key elements for implementing Zero Trust security using a cloud-based IT architecture are described below.

- Authentication is the first element. Recent cloud use shows that cloud systems without multifactor authentication experience a very high likelihood of unauthorized access. Hitachi has responded by considering how best to implement cloud-based authentication and working on improving permissions management and individual user authentication.

- The endpoints are the second element. The goal here is to improve endpoints as a total system that includes cloud systems and applications as well as PCs, servers, and smartphones. Work is also being done to study the security of network gateways and the data itself.
- Cyber-integrated monitoring is the last of the three elements. The focus has traditionally been on analyzing and responding to logs in perimeter-based networks. However, the years ahead are going to see a need to respond to incidents by gathering and analysing the correlation among a wide range of logs from the cloud, endpoints, and other components. So the company has started studying monitoring systems and organizations created as refinements of conventional cybersecurity monitoring.

As mentioned above, threat actors are targeting new industries, using higher-pressure tactics to escalate infection consequences and to render trusted detection methods too slow. This is the reason why cyber security investments have been considerably increasing in the past years, nonetheless the number of successful cyber-attacks continues to increase steadily.

Based on Zero Trust security, PATECCO IAM solutions support organisations and businesses reduce the surface of attack and provide a parallel way of stepping forward when existing line of defence does not deliver.

About PATECCO

PATECCO is a privately held German company providing services in the areas of the development, implementation, and support of Identity & Access Management solutions.

The company delivers comprehensive solutions based on latest technologies such as Cloud Access Control, Privileged Account Management, Managed Services, Access Governance, Identity Governance and Intelligence, Role-Based Access Control, Security Information and Event Management, Recertification and Asset Management. Its long-term partnership with IBM supports the success in a number of international consulting projects.

CONTACTS

PATECCO GmbH

Tel.: +49 (0) 23 23 - 9 87 97 96
Ringstrasse 72 - 44627 Herne
E-Mail: info@patecco.com
www.patecco.com