PATECCO
dynamic identity systems.

September 2020

PATECCO Identity and Access Management Solutions in The Era of Digital Transformation

WHITEPAPER

- Cybersecurity
- Data Breach
- Remote work
- Artificial Intelligence

Table of Contents

1.Introduction

Digital transformation refers to different thinking, innovation and change of the current business models. This is possible by building up a digital strategy which is able to improve the experience of your organization's employees, customers, suppliers, and partners. For the establishment of the new business and digital strategies, organizations need a strong IT infrastructure that supports all the upcoming changes with agility, productivity and security.

In the last several years a lot of organizations started their digital transformation, using Identity and Access Management technology. It ensures not only a safe and successful digital journey, but at the same time brings successful customer and employee experience.

Why IAM?

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.

According to Gartner, IAM is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons. Therefore, the lack of a proper IAM process in place, puts the data at risk and this situation may lead to regulatory non-compliance or even worse – a data breach event. IAM addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet all rigorous compliance requirements. This security practice is a crucial measure for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.

Talking about transformation in the digital era, it is crucial for the companies to develop long-term technology infrastructure plans that inform how identities are established, maintained, secured, leveraged by applications and distributed within and out of an organization. That means that the major IAM themes in the enterprise's strategy should include Privileged Access Management, Identity and the Internet of Things, Cloud-based IAM, Identity Governance and Customer IAM.

Which are the main IAM advantages in the digital transformation?

1. Ability to manage digital identity for accessing information and resources

Identity and Access Management solutions provide the ability to manage digital identity for accessing information and resources. That means that they secure content from unauthorized access by injecting authentication layers between the users and the critical apps and data. Protected target resources may include on-premises or SaaS applications and web service APIs across all business scenarios, from business-to-employee (B2E) to B2C. Besides, Identity and Access management solutions support bring-your-own-device (BYOD), through the use of social identity integration needed for registration, account linking and user authentication.

2. Ability to quickly enable access to resources and applications

According to our partner, IBM, IAM technology quickly enable access to resources and applications, whether in the cloud, on premises, or in a hybrid cloud. Whether you're providing access to partner, customer or employee-facing applications, you'll be able to offer the seamless experience your users expect.

3. Ability to simplify activities

Creating an identity-focused digital transformation strategy means choosing the right technologies that enable internal or external users to streamline actions, duties, or processes. When you create a strategy intending to enable users, you need to focus on which identities need access to the technology, how they use the technology, what resources they need and most important – how to control their access to prevent unauthorized access.

You are on the right way if your strategies closely align with the purpose of an IAM program. IAM and IGA (Identity Governance and Administration) programs define who, what, where, when, how, and why of technology access. When composing your enterprise digital transformation strategy based on an identity management program, you are ready to successfully manage the data privacy and security risks.

As mentioned above, IAM is a critical element of the digital transformation which makes it substantial for protecting sensitive business data and systems. When implemented well, IAM provides confidence that only authorized and authenticated users are able to interact with the systems and data they need to seamlessly do their job. Effective IAM solutions include Access Management – a solution that streamlines and manages multiple accesses, as well as Identity Governance and Administration – a solution that helps you monitor and govern the access.

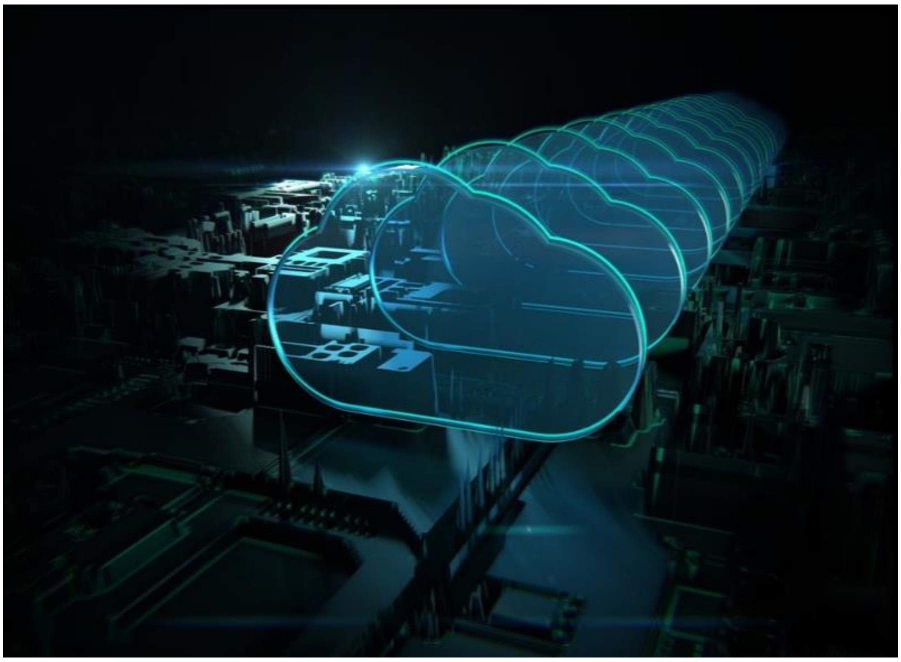
2. The Role of Identity and Access Management in Cybersecurity

In today's digitally transformed world, Identity and Access Management (IAM) plays an essential role in every enterprise security plan. As the business stores more and more sensitive data electronically, the need to protect sensitive information and data becomes critical. In this sense, IAM solution gives or limits the access permissions of different employees according to their roles.

Why IAM becomes more important than ever for enterprises?

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.

Identity and Access Management is a Cyber and Information security discipline that ensures the right people have appropriate access to the organization's critical systems and resources at the right time. For that reason IAM is based on three major pillars (Identification, Authentication and Authorization) which prevent the company to be exposed to cybersecurity threats like phishing, criminal hacking, ransomware or other malware attacks.



Benefits of IAM solutions having a significant influence in the cybersecurity

As mentioned above, effective IAM infrastructure and solutions help enterprises establish secure, productive, and efficient access to technology resources across these diverse systems while delivering several important key benefits:

IAM enhances security: This is perhaps the most important benefit organizations can get from IAM. Consolidating authentication and authorization capabilities on a single centralized platform provides business and IT teams with a streamlined and consistent method of managing user access during identity lifecycle within an organization. For example, when users leave a company, centralized IAM solution gives IT administrators the ability to revoke their access with the confidence that the revocation will take place immediately across all the business-critical systems and resources which are integrated with centralized IAM solution within the company. Thus, by controlling user access, companies can eliminate instances of data breaches, identity theft, and illegal access to confidential information.

Reduced Security Costs: Having a centralized IAM platform to manage all users and their access allows IT to perform their work more efficiently. In the digitally hyperconnected world, employees have access to hundreds of systems and resources as part of their job. Efficient centralized IAM solution can successfully address this challenge which results in huge savings of time and money for the company. A comprehensive IAM solution can reduce overall IT costs by automating identity processes that consume IT resources, such as onboarding, password resets and access requests, eliminating the need for help desk tickets or calls. Whenever a security policy gets updated, all access privileges across the organization can be changed in one sweep. IAM can also reduce the number of tickets sent to the IT helpdesk regarding password resets. Some systems even have automation set for tedious IT tasks.

IAM Provides direct connectivity: Connectivity is a hallmark of IAM because it provides direct linking to more than one hundred systems and applications. Supporting a wide range of systems, IAM makes it possible not only to apply Workflow Management and Self-Service to user account management, but also to a variety of other service provisioning processes including: requesting physical access to a work area, applying for a smartphone, or submitting a helpdesk ticket.

Least Privilege Principle: Least privilege is an important practice of computer and information security for limiting access privileges for users. With the increasing number of data breaches involving an insider, it is necessary to ensure access to all your corporate resources are secured and granted using least privilege principle. In a company it is a common practice for employees to move across different roles in the organization. If the granted privileges are not revoked when the employee changes the role, those privileges can accumulate, and this situation poses a great risk for many reasons. That makes this user an easy target for cyber hackers as his excessive rights can be an easier gateway for criminals to access the broader part of the company's critical systems and resources. Or this can eventually turn into the insider threat where a person gets the ability to commit data theft. Sometimes companies forget to remove these excessive privileges from a user's profile when he or she leaves the company. That leads to a security risk where the user can still access the company's systems even after the termination. In this case, a well-designed centralized IAM solution can help organizations eliminate insider threat challenge by utilizing the Least Privilege Principle to a great extent. Ransomware or other malware attacks.

3.Why Identity and Access Management Is So Important In Preventing Data Breaches?

For better optimization of efficiency, agility, and to drive greater collaboration, it is essential for the enterprise to be able to share information, resources, and applications with external value chain partners in a trusted way. This article explores how Identity Access Management (IAM) provides the policies and processes for ensuring that the right people in the company have the right access to secure resources, at the right time, while improving security, productivity and visibility.

Identity Is Core To Data Security

In the era of globalization, enterprises are undertaking significant digital transformation initiatives to integrate more applications and automate processes to increase productivity and innovation. These initiatives frequently involve the integration of information technology with operational technology, even bridging security domains, through direct integration with value chain partners. Digital transformation initiatives deliver significant value, but potentially put more resources at risk and increase the enterprise security threat surface.

Moreover, enterprise managers require visibility into the organizations and must be able to delegate administration of people and resources to trusted individuals within the supplier organization if they want to have the agility they need. At the same time, they must be able to govern those external users are authorized to do. This practice requires regular processes where delegated administrators attest to users' validity and the resources to which they have access for a complete audit trail and to ensure compliance.

At its core, Identity and Access Management ensures that a user's identity is authenticated to a high degree of assurance, and that the user is authorized to access the right services he or she needs. So, Access Management solutions provide authentication and authorization services and enforce user access policy to a company's employees and customers across the web, mobile apps, and other digital channels. According to Data Breach Investigation Reports, 80% of data breaches involve compromised or weak credentials, and 29% of all breaches involve the use of stolen credentials. That means that passwords are the main point of vulnerability and the more frequently you have to request or change access for lost or forgotten passwords, the larger is the risk for your personal and professional data to be hacked.

When applied properly, advanced Identity and Access Management tools can help detect suspicious activities quickly whether they are committed by external or internal criminals. In fact, insiders who have highly privileged access pose the greatest risks as they may be disgruntled or have financial problems, therefore have the incentive and opportunity to commit a perfect crime. Highly technical users who have privileged access can also cover their tracks by modifying system logs. Sometimes, users also make mistakes and errors which can also be mitigated with IAM capabilities such as Multifactor-authentication and Role-based Access Control.

Products like Microsoft Identity Manager (MIM 2016) is able to synchronize identities between directories, databases and applications, which means that employees' identities are managed wherever they are working from. It also provides increased admin security with policies, privileged access management and roles. This, combined with Microsoft's Azure Active Directory (AAD) technology, provides additional cloud based self-service capabilities, secure remote access, single sign on, and multi-factor authentication.

How Can IAM Practices Prevent a Data Breach?

Automating the access privilege provision

For every new employee addition, you should assign all the privileges based on their roles and business rules. It's better to have workflow automation. Besides, for every employee resignation or termination, you must ensure that all the privileges will be taken away automatically. This practice will help in limiting and preventing unnecessary privileges.

Privileged User Management

Basically, the organized attacks target the privileged accounts of the organization. Once a privileged account gets compromised, it increases the chances of a massive security breach. Social engineering and phishing attacks are some common ways of tricking privileged users in sharing their passwords. Such attacks can remain undetected for a long period and that is why it is recommended to implement privileged user management. Any access considered privileged should be assigned to a separate account within the system for which the access is granted, and such accounts should be assigned to the user after an appropriate review of the user’s duties and justification for both the privileged account and the specific access. Any privileged access defined or granted should be limited in both scope and the number of users to which it is assigned and tailored to the needs of the business.

Account and access reviews

A useful practice is to conduct Account and access reviews. This can be done periodically in smaller companies and even in larger companies, as well. For example, if a user changes jobs, you should trigger an access review based on changes in the user’s job code or department code. Access reviews can also be based on risk, or when users request certain types of access, i.e., conduct a review of all of user’s access if the user requests domain administrator access, or if a user’s risk score reaches a certain level. Access reviews should be done either by the entitlement owners, or the current manager.

Entitlements warehouse

It is a good approach to set up an entitlements warehouse, which identifies all the entitlements in all the systems within the organization, who is assigned to those entitlements, and includes risk rating and privileged access flags for each entitlement. The entitlements warehouse can also be used to conduct peer analytics to identify unusual patterns of entitlement assignments based on entitlements assigned to other users with similar job functions, or assigned to users in similar or the same department.

Compliance

Another reason why Identity and Access Management is important in preventing data breaches is because organizations must comply with increasing, complex and distributed regulations, and they must ensure and demonstrate an effective customer identification process, suspicious activity detection and reporting, and identity theft prevention. Identity and Access Management solutions can be leveraged to manage various regulatory requirements such as having a Customer Identification Program (CIP), Know Your Customer (KYC), monitoring for Suspicious Activity Reporting (SAR), and Red Flags Rule for identity fraud prevention.

Identity and Access Management is regarded as complex and critical solution in managing security risks. Although technology is an important part of identity and access management which can be leveraged to support an organization’s cybersecurity objectives and strategy, effective IAM also requires processes and people for user onboarding and identity verification, granting and removing access, detecting suspicious activities, and keeping unauthorized users out of the systems. IAM can help organizations achieve operating efficiency and optimal security through advanced technology and automation such as adaptive, multi-factor, and biometric authentication.

4. Which Key IAM Capabilities Successfully Support Remote Work

The coronavirus pandemic has overturned normal ways of working. Many office workers are based at home for certain period of time and apply new methods and practices to accomplish their daily tasks. Staying connected to colleagues and partners seems so easy and functional, but remote working brings a lot of challenges when it comes to cybersecurity.

With the increase of the online activities, traditional IT environments and Identity and access management (IAM) systems are being pushed to their limits. All that leads to latency, frustration, friction, and increased risk, making organizations to search solutions of how to support business at scale without compromising security and user experience.

Identity as a tool for preventing cyber threats

We assume that your company has already started to work remotely – with policies to support the practice and an analysis of expected traffic and risks. So, in this article we will cover some of the most popular IAM capabilities on which medium and large enterprises trust in today’s complex business world. The primary cybersecurity tool they can use to prevent data breaches is Identity and access management. It is also considered as the true digital perimeter, ensuring that only trusted parties can enter the corporate network. It is also a fact that Identity and access management is able to make the transition to a remote workforce easier by securely connecting employees to their work, all while IT maintains complete control.

Identity, more specifically identity authentication, now forms the digital perimeter once composed of antivirus solutions. This digital perimeter serves as the main mechanism by which threat actors are kept out. Even if they do penetrate the perimeter, identity can constrain their permissions, limiting the damage they inflict on your network. Moreover, identity also provides critical information for other cybersecurity solutions, including SIEM and Endpoint Security. Identity informs and strengthens user and entity behaviour analysis and recognizes, stores, and monitors device identities. Both can help prevent external threat actors from penetrating your network or recognizing insider threats before they unfold.

Which key IAM Capabilities help to maintain complete visibility and control over employee access?

No matter where the team is working, IAM has several key capabilities that can make the transition to a remote workforce easier by securely connecting employees to their work, all while IT maintains complete control.

Authentication

When your workforce is enabled to access corporate resources, the first step is to validate the user's identity. Authentication has a number of risks related to the method of access, from simple passwords to a layered approach with two-factor, VPN and threat detection. Talking about remote workers, using remote devices and getting remote access, there are a few things to have in mind when enabling their authentication:

First – do you already have strong authentication in place today? Our advice here is to protect that investment and to expand its capability by getting more licenses, capacity and management. You should also identify critical applications and make sure passwords are secure. If you have apps that your business needs to function and will be accessed remotely, add layers of authentication to these first. In case the users use passwords to access applications, add Multi-Factor Authentication tools, as well.

Second – it is a good practice to force a password change more often, especially when users go remote. Update your company password policy to show users what they need to do, and increase the password requirements to make them stronger.

Third – do not forget to create network/location aware remote access policies that ensure stricter passwords or host information profiling to gain access.

And last – constantly monitor user access to critical systems and make sure you can make sure who is actually logging into the systems so that any threats could be prevented.

Authorization

After authentication, the authorisation is the most critical layer to IAM. Each company has a different way to authorize users based on its industry, business model and culture. But there are some basics that should be considered to make sure remote workers are enabled and secure:

Make sure you have an approved corporate policy in place that spells out what employees should have access to, including data classification and what data can and cannot be shared or stored on remote devices.

If you have an identity governance tool in place, use those tools to enforce roles and what applications users should have access to.

Centralize your identities into one directory infrastructure for better control and harden their operating systems of the critical applications.

Creating a Zero Trust architecture and program is also a good idea, because in this way not only users must be authenticated and authorized, but also applications, systems, networks, IoT devices and data.

Implement Privileged User Management (PAM) and Databases Access Management (DAM) to lock down those critical administrator accounts. Enable them with tools, but secure them with controls.

Administration

The daily administration of users is the first mismanaged area in IAM when a crisis comes. The best solution in such situation is to automate administration as much as possible, so that enforcement and security risks are not underestimated.

What needs to be done is to force users who need access to a critical system to formally request that access through a help desk ticket. Then it is recommended to update your firewall policies with the service ticket number and to review by date.

The next step is to audit what users have access to before you allow them to work from home. Let the users justify what access they have and remove anything they don’t need. This process is connected to least privilege in IAM. Based on that, we can make a conclusion that access to critical applications and data needs to be properly managed and to ensure that threats are discovered and successfully handled.

Identity and Governance enhanced by AI and ML

As mentioned above, in recent times a lot of organizations support their entire workforce remotely. Identity Governance and Administration helps you manage and provision user access, as well as reduce the risk that comes with employees having excessive or unnecessary access to applications, systems, and data. Machine learning (ML) and artificial intelligence (AI) take IGA to the next level by automating the most common activities. This process includes automatic approval of access requests, performing certifications, and predicting what access should be provisioned to users. The modern IAM platforms, which are enhanced by Artificial Intelligence and Machine Learning, increase efficiency and provide more time for IT staff and access approvers to focus on access rights that have been identified as risky or anomalous. The result is increased security and decreased administrative burden.

Thanks to the modern IAM capabilities, each organisation can easily address the demands for remote work, study, and play at scale. Now more than crucial for the business is to be well prepared and able to meet the challenges of the digital transformation and the global crisis, as well.

5. Key Aspects of an Identity Access Management Strategy

The components and functionalities of identity and access management bring a lot of benefits to all users who are involved into the organisation's ecosystem, no matter of the business sector they belong to. Before engaging yourself to an IAM project, it is critical to determine and to have a long-term vision of your IAM strategy. This initiative is much more effective and profitable than having to assemble various solutions that may not be appropriate or not always well integrated.

A clear identity and access management strategy is fundamental for organisations to operate effectively. It will guarantee secure access to the information system, ensure compliance with regulations, reduce a large number of operating risks, improve productivity and the quality of service delivered to users. Many organisations' failures prove that fact that the lack of expertise and effective identity and access management strategy can led to risky implementations and expensive mistakes. This is the reason why many organizations look for experienced service providers for assistance.

Building an Identity and Access Management Strategy

1. Discovery Is the First Step

The first step in developing an IAM strategy is to gain a thorough understanding of the customer's current state. This step is crucial, because an accurate picture of an organization's current state helps to create a more realistic strategy and results in successful project implementation. There are three ways to develop a better understanding of the customers' current environments, needs, and goals.

Understand the How. To better prepare and develop context before beginning a project, you should search for specific artifacts and documents that help understand how the organization functions. That could include any existing IAM policies and procedures, IAM architectural diagrams, relevant audit findings, and an overview of the network and server environments. It is also helpful to get to know the current technology elements: which are the main applications and systems being used, and how they are set up and customized.

Understand the Who. Developing a demographic profile of the organization is also very important, i. e – how many users there are, what is their location, and who gets access to what. Viewing the structure of the organization is also essential: who approves access requests, which users are employees or non-employees, and how HR interacts with the existing IAM process.

Understand the Why. Understanding the drivers for an organization's IAM project is pivotal for the project's success. It ensures that leaders are on the same page about their reasons for investing in IAM, sets clear expectations for the project's outcomes, and helps champions justify the project internally.

2. From Discovery to Deliverables

When the discovery process is finished, the next step is to conduct an analysis of what you have collected as an information. For some companies, this means a roadmap and a strategy, but others might need a competitive assessment, an IGA recommendation, or advice on the best way to handle role-based access. Here are some examples of the deliverables that can be provided:

Architecture. A smart approach is to develop a map that captures how IAM currently functions at the organization and represents all the systems, architecture, tools, users, and connectors. This map should accurately reflect the organization's environment, processes, patterns, and challenges. On the basis of this "big picture" of the organization's current state, an architecture that reflects the ideal state could be created.

Roadmap. The roadmap describes the actions which companies need to take to get from A to B, and helps companies prioritize these actions and put them in the appropriate order.

Tool Recommendations. With a clear understanding of the customer's requirements and extensive knowledge about the best tools for every situation, the needs to the appropriate vendors could be properly matched.

3. Perform a comprehensive audit

Another significant step is to perform a comprehensive audit of current practices so that you know exactly what types of systems or processes are used by employees to share and transfer information. You may find out that people in your organization are subverting security controls to get their work done. It's a common issue that can help you build a stronger access management structure.

4. Develop IAM Governance Procedures

It is very important to ensure that risk management and compliance guidelines are followed consistently throughout the company. That could be verified by efficient provisioning and de-provisioning procedures. Besides, the privileged accounts should be handled with care. Compared with accounts for regular users, these accounts can have almost unlimited access to sensitive data, applications, and devices. You should strike a balance between access and security by following the guidelines of least privilege. When users need elevated privileges for a specific task, it is recommended to grant access for a limited time using unique credentials.

5. Compliance is a top consideration

Its crucial to ensure that compliance guidelines and risk management are incorporated into the identity management strategy. Privacy management and data access governance is an important aspect of IAM. It controls who is capable of accessing user data and how they can share or use it. This ensured that organizations meet the growing requirements of changing industry and global data privacy regulations like the General Data Protection Regulation (GDPR).

6. Add Cloud-based IAM to Your Arsenal

If you are looking to the cloud for greater efficiency and easy scalability, cloud-based identity and access management services can be part of your IAM plan. Identity and Access Management-as-a-Service (IDaaS) simplifies even the most complex user management challenges. These systems exist in environments defined by strict access with regular monitoring and security for both IT and physical assets. Scheduled backups and data recovery plans prevent catastrophic losses. Further, the access control measures are certified to industry standards with frequent audits. You can meet necessary audit requirements by leveraging existing security certifications rather than investing talent and resources within a similar internal plan.

IAM projects are complex, that is why a defined strategy for success is required. Without a good IAM strategy, analysis and planning the projects usually fail. A successful IAM strategy balances security requirement with employee and customer experience and communicates these goals effectively to executives.

PATECCO is your partner through all phases of IAM strategy: Our practice is to work closely with your technology management and business leaders and to consult you for the sequence of projects needed to make your strategy a reality. Whether you would like to implement a new IAM strategy or update an old one, our consultants can offer their professional support to successfully build up your IAM strategy.