MANAGING IDENTITIES & ACCESS

Dexperts

TABLE OF **CONTENTS**

FACTS

In a survey by the Center for Strategic and International Studies (CSIS), **42%** of organizations reported that their cyber security incidents increased during the pandemic.

According to a study by the SANS Institute, the most common security challenges faced by decentralized organizations are endpoint security (**54%**),cloud security (**52%**), and network security (**52%**)

A report by Kaspersky, remote working increased the risk of data breaches by **66%** in 2020.

According to a study by the SANS Institute, the most common security challenges faced by decentralized organizations are endpoint security (**54%**), cloud security (**52%**), and network security (**52%**)

The 2020 Verizon Data Breach Investigations Report found that **83%** of breaches involve weak, default, or stolen credentials.

A study by Deloitte found, by the end of 2022, that **55%** of companies have been targeted by a phishing attack in the past 12 months.

In a survey by the National Cyber Security Alliance, **60%** of small businesses that experience a cyber attack are out of business within six months.

WHY INVEST IN **CYBER SECURITY?**

All the modern enterprises are decentralized. Decentralized organizations and businesses, also known as distributed organizations, are those that have a decentralized structure with multiple locations, remote workers and contractors, and third-party partners. The connection with these end points in the distributed organizations are not one to one. Rather, each of these end points are connected to many other nodes within the organization and outside the organization. These multi-tired relationships can be complex, complicated and unique. As the organization needs to move towards automation and globalization, these interdependencies tend to increase more. And to remain connected with all the various components, the organizations need to be heavily dependent on the cyber infrastructures. Thus, these organizations are vulnerable to a wide range of cyber threats, including phishing attacks, ransomware attacks, advanced persistent threats, network-based attacks, and insider threats.

Cyber security becomes absolutely critical for decentralized organizations to help it protect sensitive data and systems from unauthorized access, breaches, and other cyber threats. For the optimal efficient and productive collaboration among these multilevel partnership a secure and versatile information sharing is required.

Secure as in, all the parties must have trust when exchanging sensitive data and resources. Versatile, the parties should be able to easily integrate into the organization without much friction to burn their existing setups.

Investing in cyber security enables organizations to comply with regulations and industry standards that require strong authentication and access controls, which makes it easier for all the stakeholders involved to trust any data and resource exchange. It enables organizations to improve productivity and reduce costs by automating many of the manual tasks associated with managing identities and access. It also gives organizations better control over access to their resources, which helps to reduce the risk of data breaches, theft, and other security incidents. A comprehensive cyber security strategy that includes technical controls, Identity, and Access Management solutions, data encryption, employee education, and regular security audits can help organizations to reduce the risk of cyber-attacks and protect against data breaches, theft, and other security incidents.

Cybersecurity is not just an IT problem, it's a business problem. It's not just about protecting data, it's about safeguarding reputation, revenue, and relationships.

And, Information and Access Management (IAM) is the cornerstone of cybersecurity. It's the first line of defense against cyber threats, and if done right, it can prevent most attacks before they happen.

WHAT IS
IDENTITY & ACCESS MANAGEMENT?

That is an oversimplified explanation, but the core idea of Identity and Access Management (IAM) is that it is a cybersecurity discipline that enables the right individuals to access the right resources at the correct times and for the right reasons.

With IAM principal organizations set up a security framework that enables organizations to control access to their resources, both in the cloud and on-premises. It allows businesses to manage and secure access to their applications, data, and infrastructure by creating and ordering identities, such as users and groups, and by defining permissions for those identities to access resources.

All the entities, including people and applications, are defined as identities. These identities will need correct privileges to access any of the resources. IAM enables organizations to implement a principle of least privilege, which means that users are only granted the permissions they need to perform their job tasks. This helps to prevent unauthorized access and data breaches.

WHY NEED
IDENTITY & ACCESS MANAGEMENT ?

"Identity and Access Management is the foundation of security, without it, an organization is simply building castles in the air."

IAM is a crucial component of an effective security strategy for any modern organization. It is not only the frontline of cyber defense for any multi-tiered decentralized organizations but IAM implementation also becomes necessary for other several reasons too:

Protecting sensitive data: IAM helps organizations to protect sensitive information and systems by controlling access to resources based on user identities and roles. This helps to prevent unauthorized access, data breaches, and other security threats.

Compliance: IAM can assist organizations in meeting various compliance requirements such as HIPAA, GDPR, and SOC 2 by providing the necessary controls and processes to secure sensitive data.

Managing remote workforce: With the rise of remote working, IAM solutions can help organizations to manage and secure access to resources for remote employees and contractors, ensuring that only authorized individuals have access to sensitive resources.

Managing third-party access: IAM is also important for controlling access to resources by third parties such as partners, vendors, and customers. It can help organizations to ensure that only authorized third parties have access to the resources they need to do their jobs while preventing access to resources that they don't need.

Improving productivity: IAM is also important for controlling access to resources by third parties such as partners, vendors, and customers. It can help organizations to ensure that only authorized third parties have access to the resources they need to do their jobs while preventing access to resources that they don't need.

Reducing costs::IAM can help organizations to reduce costs by automating many of the manual tasks associated with managing identities and access, such as provisioning and de-provisioning user accounts.

Hence, for these reasons IAM becomes absoultly important across domain and industries. Enterprises and businesses of all sizes, from small start-ups to large multinational corporations,Government agencies and municipalities, Non-profit organizations and educational institutions, Healthcare providers and hospitals, Financial institutions and banks, Online retailers and e- commerce businesses, Cloud service providers and SaaS companies and more

HOW TO GET STARTED WITH **IDENTITY AND ACCESS MANAGEMENT?**

It is important to remember that IAM is not just a one-time setup but an ongoing process that requires constant monitoring, updating, and maintenance to keep it secure and effective.

Also, as David Doret - deputy CISO at BNP Paribas and Founder of Open- Measure, famously said "IAM is so transversal within the organization - we need to work with HR, IT, security, the full workforce, top management, customers - with everyone". IAM implementation is not just the responsibility of the IT team but the entire members and parties of the organization need to get involved. Hence, the IAM implementation affects all the entities in the organization.

IAM solutions includes the following components:

AUTHENTICATION

Verifying the identity of users, devices, or systems.

AUTHORIZATION

Granting or denying access to resources based on user roles and policies.

IDENTITY MANAGEMENT

Creating, maintaining, and managing user identities and attributes.

ACCESS MANAGEMENT

Managing and controlling access to resources, such as applications and data.

AUDITING AND REPORTING

Recording and reporting on access attempts and activities for compliance and security purposes.

The IAM implementation strategy can be detailed as follows

Define the scope of your IAM system: This includes identifying the resources that need to be protected, the users who will be accessing them, and the roles and permissions that will be assigned to those users.

Choose an identity provider (IdP): This could be an existing system such as Active Directory or LDAP, or a cloud-based service such as AWS Cognito or Azure Active Directory.

Configure the IdP: This includes setting up user accounts, groups, and roles. It also includes configuring the IdP to work with your organization's existing authentication methods, such as password policies and multi-factor authentication.

Integrate the IdP with your applications and services: This could involve configuring your applications to use SAML, OAuth, or OpenID Connect for authentication and authorization. It also includes configuring your applications and services to use the IdP's user accounts and roles for access control.

Implement access controls: This includes setting up roles and permissions for users, as well as implementing multi-factor authentication (MFA) to further secure access.

Monitor and audit access: This includes logging user activity, regularly reviewing logs to detect and respond to any suspicious activity, and implement security measures such as intrusion detection and prevention systems.

Continuously update and improve your IAM system: This includes keeping software up-to-date, regularly reviewing and updating policies, and continuously monitoring for security threats.

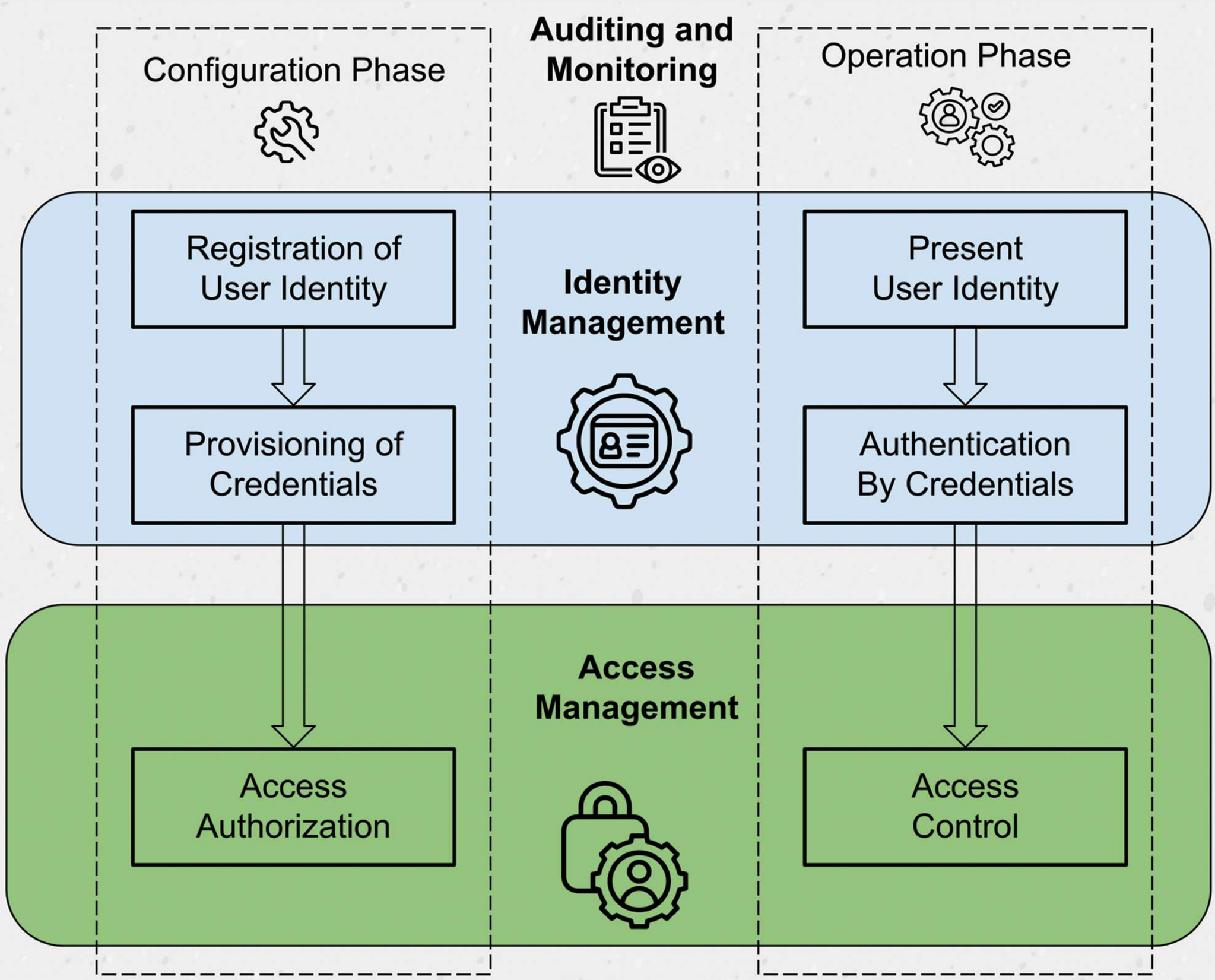
Test the system: Conduct tests to ensure the system is working as expected, such as testing the integration of the IdP with the application, testing the roles and permissions, and testing the access controls.

Deploy the system: Once the system is fully tested and ready to go live, deploy it to the production environment.

Provide training and support: Provide training to the end-users and IT staff on how to use the system and provide ongoing support for any issues that arise.

Please note that the above-listed steps are just a general guide and the actual implementation may require more detailed steps and procedures depending on the specific requirements of your organization.

HIGH LEVEL OVERVIEW OF
IAM IMPLEMENTATION



WHICH
IDENTITY & ACCESS MANAGEMENT ?

There are several different types of IAM solutions available on the market, each with its own set of features and capabilities. Here are a few examples:

Cloud-based IAM solutions: These solutions are hosted by a third-party provider and allow organizations to manage user identities and access controls in the cloud. Examples include SailPoint IdentityNow, AWS Cognito, Azure Active Directory, and Google Cloud Identity.

On-premises IAM solutions: These solutions are installed and managed by the organization itself, and are typically used by larger organizations with complex IAM requirements. Examples include SailPoint IdentityIQ, Microsoft Active Directory and OpenLDAP.

Hybrid IAM solutions: These solutions combine both cloud and on- premises elements, allowing organizations to manage some identities and access controls in the cloud and others on-premises.

Identity as a service (IDaaS) solutions: These solutions provide a cloud- based IdP and are similar to the cloud-based IAM solutions, but are specifically designed for organizations that need to outsource their identity management.

Single Sign-On (SSO) solutions: These solutions allow users to log in once and access multiple applications and services without having to log in again. Examples include Okta, OneLogin, and Microsoft Azure AD B2C.

Access Management solutions: These solutions focus on controlling access to resources and applications, often with a focus on web-based or cloud- based applications. Examples include ForgeRock, CA Single Sign-On, and IBM Security Identity Manager.

Multi-Factor Authentication (MFA) solutions: These solutions provide an extra layer of security by requiring users to provide multiple forms of authentication, such as a password and a fingerprint or a code sent via text message. Examples include Google Authenticator, RSA SecurID, and Duo Security.

The choice of the solution will depend on the specific requirements of the organization, such as the number of users, the complexity of the organization, the type of applications and resources, and the compliance requirements, among other things.

While selecting the suitable IAM solution, some of the features that are of utmost importance to analyze are:

Identity Governance: This feature allows organizations to manage and govern user access to resources and applications, including role-based access controls, user provisioning, and access request workflows.

Identity Provisioning: This feature allows organizations to automate the process of creating and managing user accounts and access across multiple systems and applications.

Identity Analytics: This feature allows organizations to gain visibility into user access and activity, including identifying and mitigating potential security risks.

Identity Certification: This feature allows organizations to regularly review and certify user access to ensure compliance with internal policies and regulations.

Identity Access Management: This feature provides a centralized console for managing access to resources and applications, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), and access request workflows.

SINGLE SIGN ON (SSO)

IAM IMPLEMENTATION ARCHITECTURE