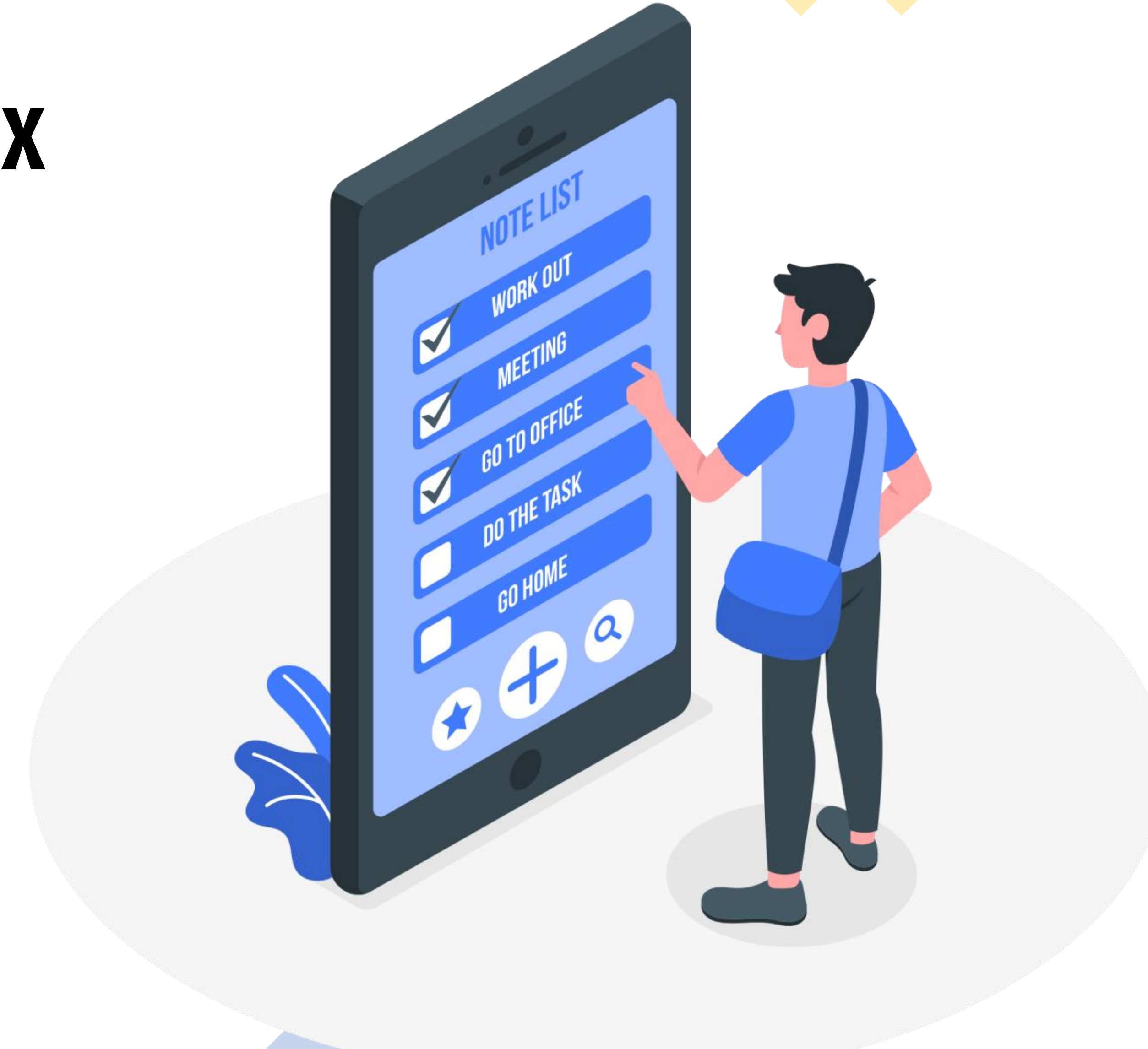
AuNEX0

IAM SOLUTION BY AUTHNEX

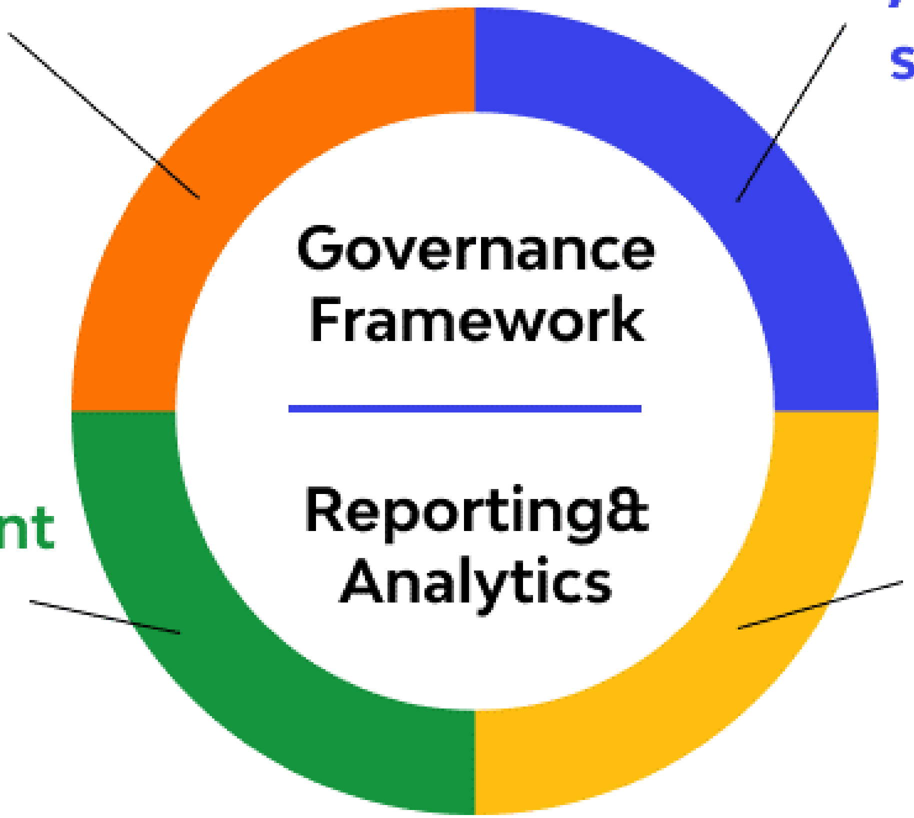
WHAT IS IAM?

IAM stands for Identity and Access Management. It is a framework of policies and technologies that ensures the right individuals have the appropriate access to resources in a computing environment. IAM systems typically manage digital identities (users, groups, roles, etc.) and their permissions to access various systems, networks, applications, and data.



The Inner Workings

IAM service components



Governance Framework

Reporting& Analytics

Authentication services

- Single sign-on
- Multifactor authentication
- Session and token managemment

Authorization services

- Roles
- Rules
- Attributes (e.g. metadata)
- Privileged access

User management services

- Provisioning
- Deprovisioning
- Self-service
- Delegation

Directory services

- Identity store
- Directory federation
- Metadata synchronization
- Virtual directory

Key Components

Authentication: Verifying the identity of users, typically through passwords, biometric factors, or multi-factor authentication (MFA).

Authorization: Determining what resources, a user or system can access after they have been authenticated. This involves setting permissions and privileges based on the user's role, group membership, or specific policies.

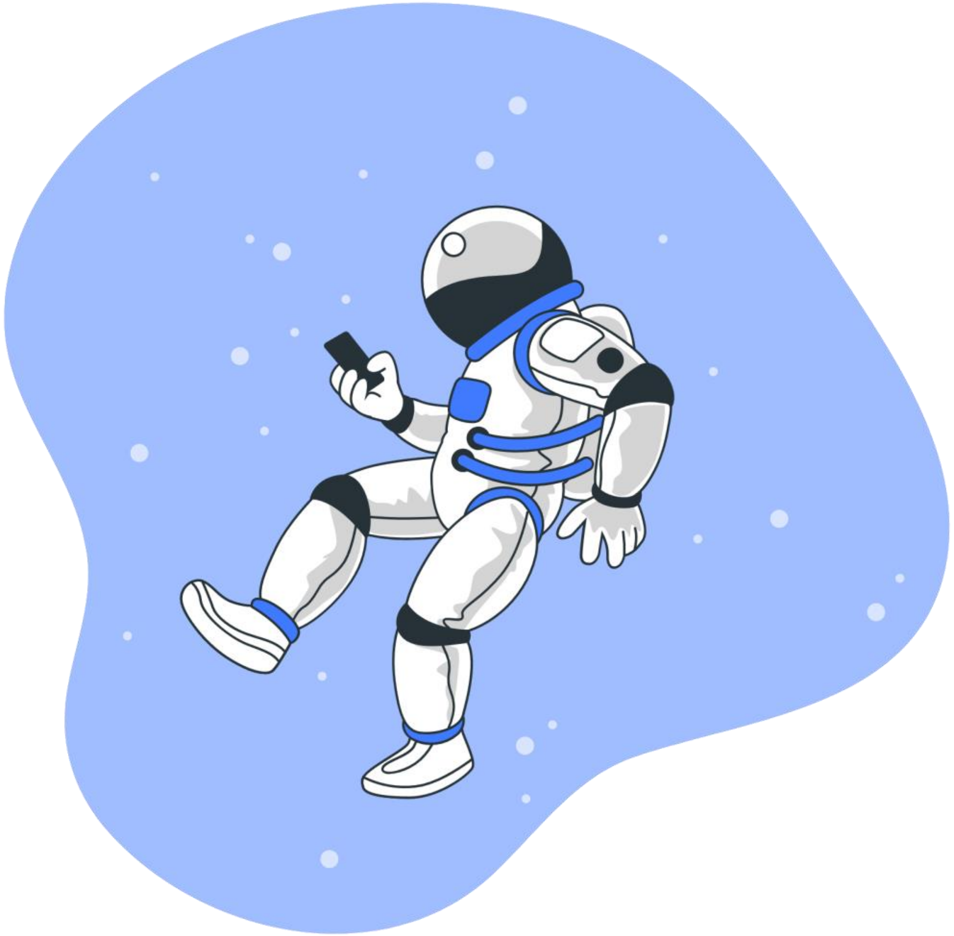
Account Management: Creating, modifying, and deleting user accounts, as well as managing their associated permissions and attributes.

Single Sign-On (SSO): Allowing users to access multiple applications or systems with a single set of login credentials.

Identity Federation: Establishing trust relationships between different identity management systems to enable users to access resources across multiple organizations or domains.

Audit and Compliance: Monitoring and logging user activity to ensure compliance with security policies and regulations, as well as for forensic purposes.

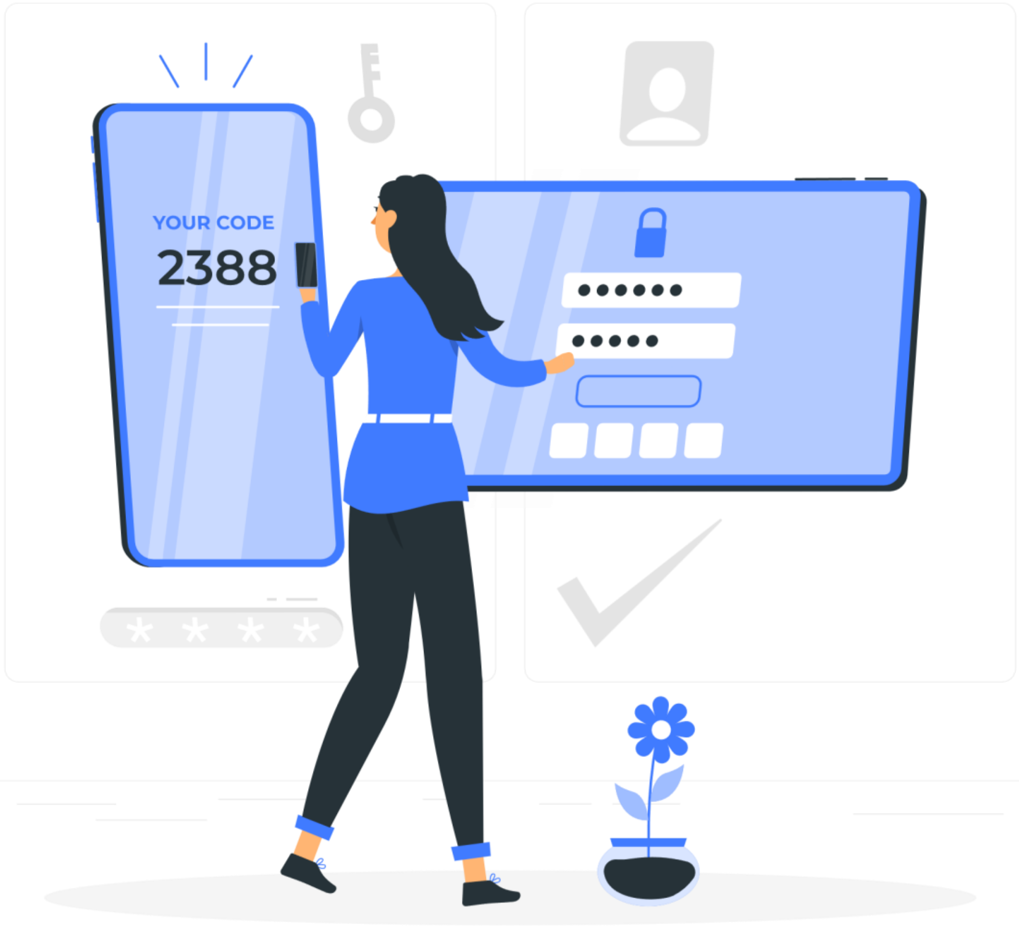
Why IAM ?



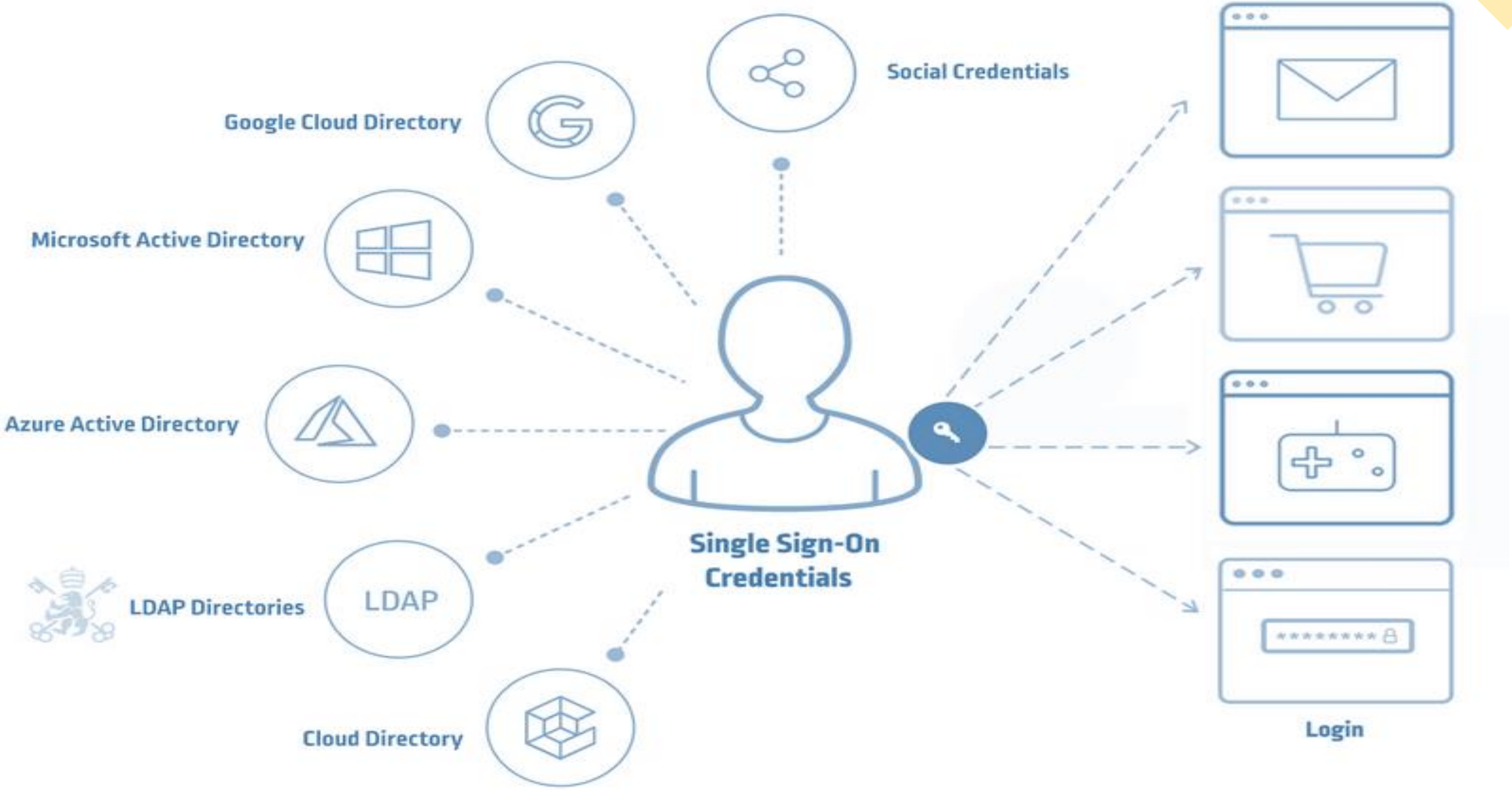
With all the bells and whistles, this seems like a fancy piece of technology…!
But why should I buy it…?

Why IAM, in les than 10 words.

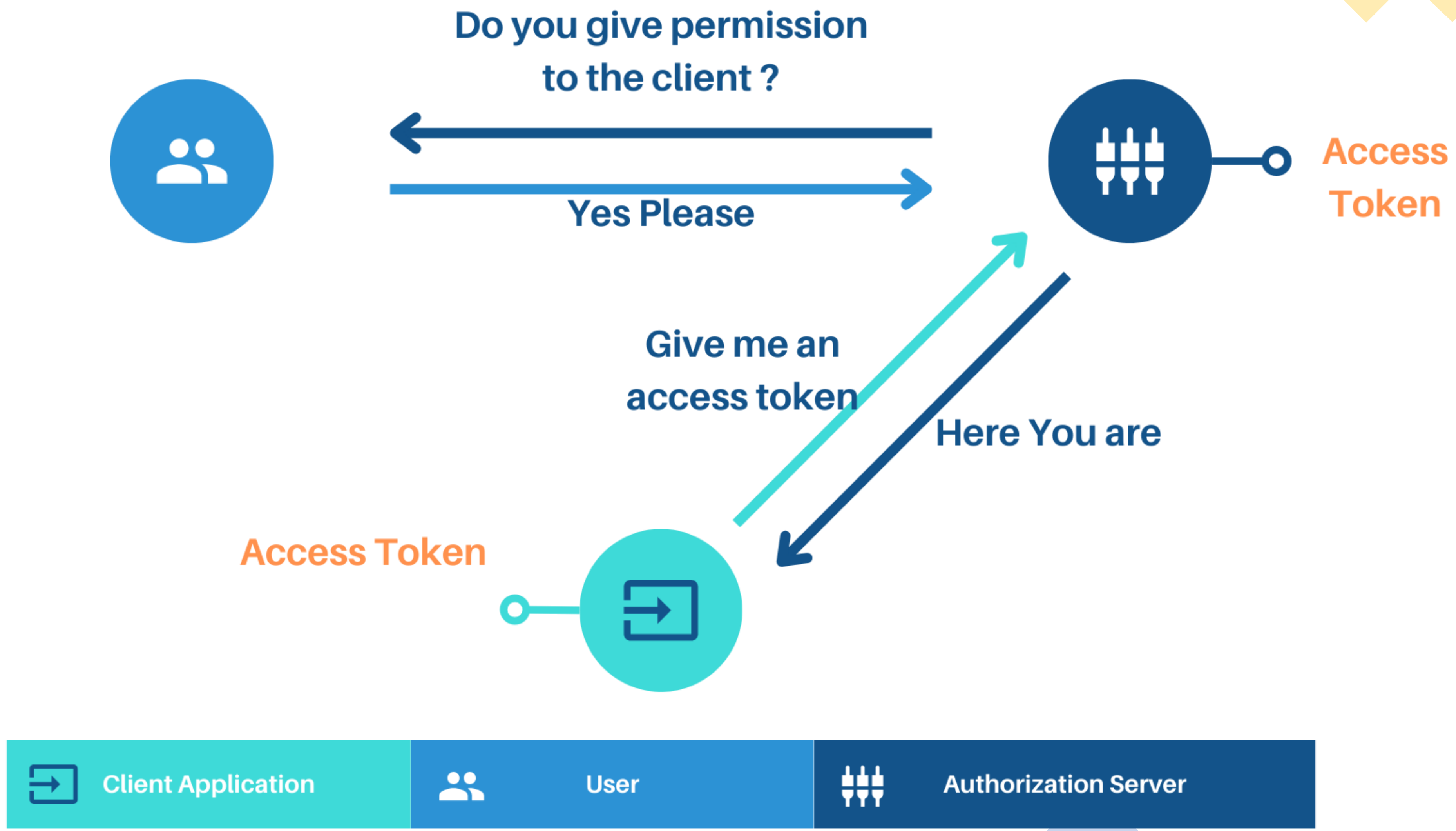
Right ***Individual***
Right ***Resource*** at
Right ***Time*** For
Right ***Reason***



Right ***Individual,*** Right ***Resource*** at Right ***Time*** For the Right ***Reason***



HOW IT WORKS



Do you give permission to the client ?

Yes Please

Access Token

Give me an access token

Here You are

Access Token

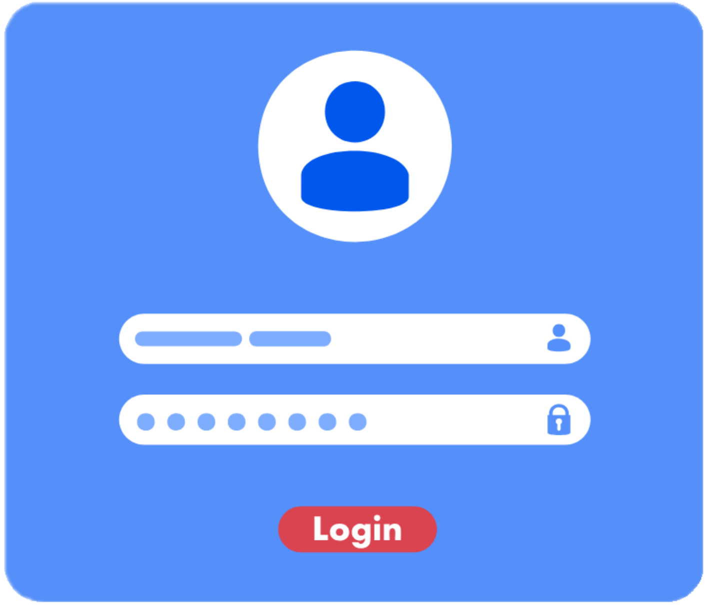
Client Application

User

Authorization Server

Authentication vs Authorization

Authentication



Who are you?

Authorization

Can you do that?

ADVANTAGES OF AN IAM

Security: IAM systems ensure that only authorized individuals have access to specific resources and data within an organization's network. By managing identities, authentication, and authorization, IAM helps prevent unauthorized access and protects against data breaches, insider threats, and other security risks.

Compliance: Many industries are subject to regulations and compliance standards that require organizations to implement strong identity and access controls. IAM systems help organizations adhere to these regulations by providing audit trails, enforcing access policies, and ensuring data privacy.

Efficiency: IAM systems streamline the process of managing user identities, access rights, and permissions across an organization's IT infrastructure. This improves operational efficiency by automating user provisioning, deprovisioning, and access requests, reducing administrative overhead and IT costs.

User Experience: IAM systems can enhance the user experience by providing single sign-on (SSO) capabilities, allowing users to access multiple applications and services with just one set of credentials. This improves productivity and reduces the burden of remembering multiple passwords.

Risk Management: IAM systems help organizations mitigate risks associated with identity-related threats, such as identity theft, credential sharing, and unauthorized access. By implementing strong authentication methods, enforcing least privilege access principles, and implementing multi-factor authentication (MFA), IAM systems help organizations better manage and mitigate these risks.

MULTIFACTOR AUTHENTICATION

WHAT IS MFA?

A multifactor authenticator, often referred to as multifactor authentication (MFA), is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or transaction. It adds an extra layer of security beyond just a username and password.

MULTIFACTOR AUTHENTICATION

YOU WILL NEED...

Something you know

This is usually a password or PIN.

Something you have

This could be a physical device such as a smartphone, a security token, or a smart card.

Something you are

This refers to biometric characteristics like fingerprints, facial recognition, iris scans, or voice recognition.

ADVANTAGES OF MFA

Increased Security: Passwords alone are vulnerable to various attacks such as phishing, brute-force, and credential stuffing. By adding an extra layer of authentication, MFA significantly reduces the risk of unauthorized access even if one factor (e.g., password) is compromised.

Mitigation of Credential Theft: With the prevalence of data breaches and password leaks, it's common for attackers to obtain usernames and passwords from various sources. MFA helps mitigate the impact of credential theft by requiring additional verification beyond what the attacker may have obtained.

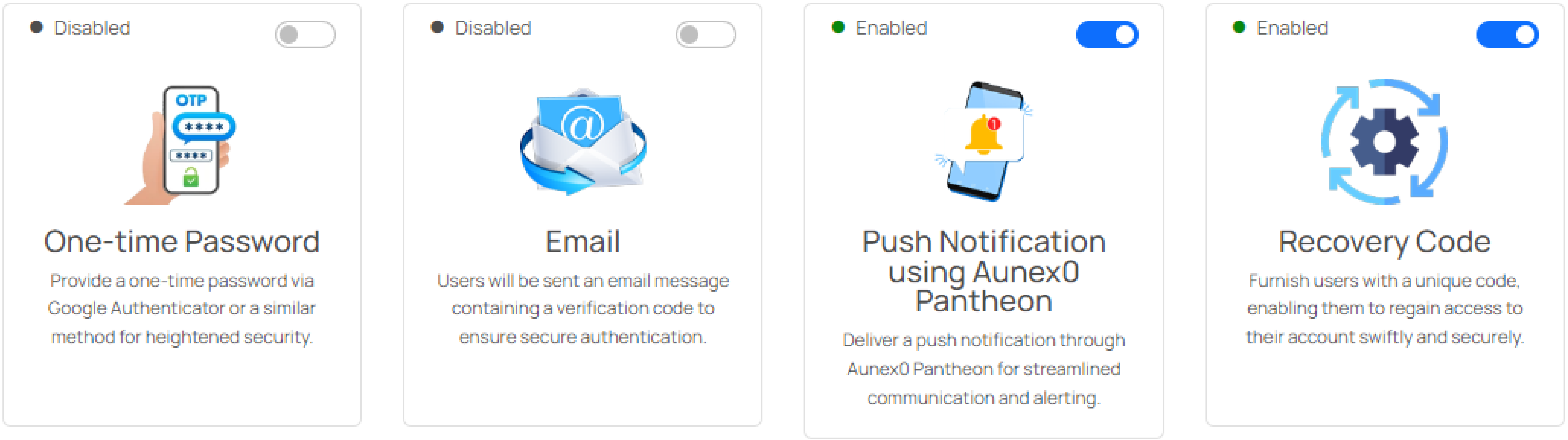
Compliance Requirements: Many industries, particularly those dealing with sensitive information such as healthcare, finance, and government, are subject to regulatory requirements that mandate the use of multifactor authentication to protect customer data and privacy.

Protection against Phishing: Phishing attacks often trick users into revealing their passwords or other sensitive information. MFA adds a layer of defense against phishing because even if a user unwittingly provides their password, the attacker will still need the additional factor to gain access.

User Convenience: While adding an extra step may seem inconvenient, multifactor authentication can often be implemented in user-friendly ways, such as through smartphone apps or biometric verification, which users may find more convenient than constantly changing passwords or dealing with the fallout of a compromised account.

Business Protection: For businesses, implementing MFA can protect not only their own sensitive information but also the data of their customers and partners. This can help preserve trust and reputation, which are critical for long-term success.

MULTIFACTOR FACTORS



● Disabled

One-time Password

Provide a one-time password via Google Authenticator or a similar method for heightened security.

● Disabled

Email

Users will be sent an email message containing a verification code to ensure secure authentication.

● Enabled

Push Notification using Aunex0 Pantheon

Deliver a push notification through Aunex0 Pantheon for streamlined communication and alerting.

● Enabled

Recovery Code

Furnish users with a unique code, enabling them to regain access to their account swiftly and securely.

WHY AUTHNEX ?

SMS Interception: Attackers can intercept SMS messages through various means, including SIM swapping, SS7 vulnerabilities, or malware on the user's device. Once intercepted, they can obtain the one-time code sent via SMS and bypass the second factor of authentication.

Phishing: Although SMS MFA requires a second factor, it doesn't protect against phishing attacks where users are tricked into revealing both their username/password and the SMS code. Attackers can create convincing phishing websites or messages to dupe users into providing all necessary information.

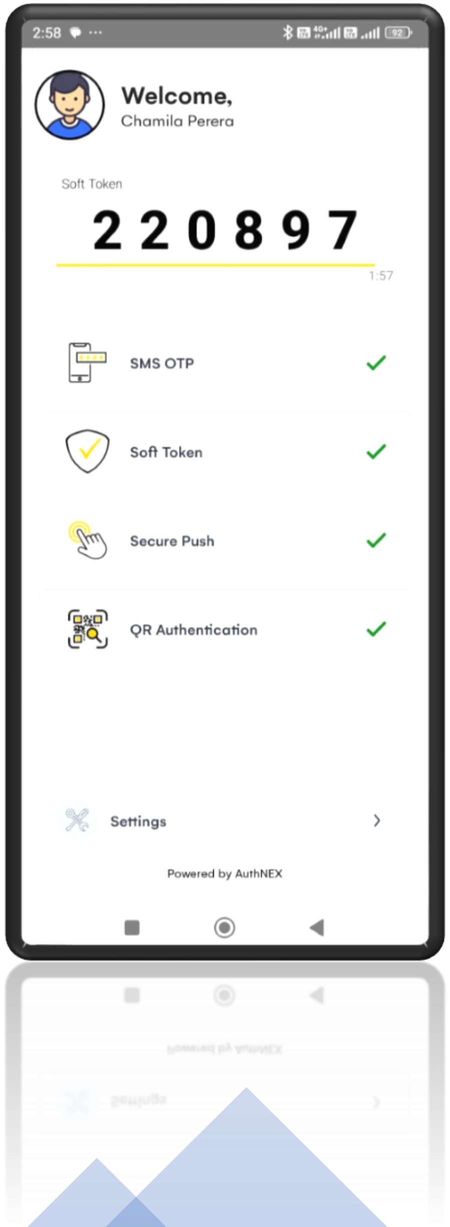
Device Dependency: SMS MFA relies on the user having access to a mobile phone to receive the SMS code. If the user loses their phone or it's stolen, an attacker could potentially gain access to both the phone and the SMS code, compromising the second factor of authentication.

Reliability Issues: SMS delivery isn't always reliable, especially in areas with poor network coverage or during network congestion. Delays in receiving SMS codes can inconvenience users and potentially hinder their ability to access services.

WHY AUTHNEX ?

What We Provide?

We offer an advanced multifactor authentication solution featuring soft tokens and push notifications as a strong authenticator. Our system prioritizes user-friendliness and advanced features for enhanced security



2:58

Welcome,
Chamila Perera

Soft Token

220897

1:57

SMS OTP ✓

Soft Token ✓

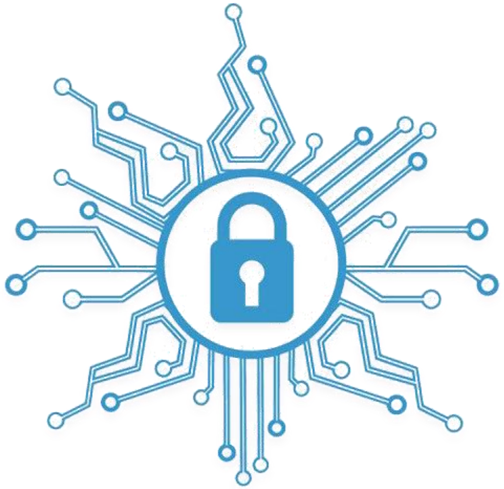
Secure Push ✓

QR Authentication ✓

Settings ›

Powered by AuthNEX

AuNEX0



Prioritizing security measures not only protects your ***AuNEX0 IAM*** application but also safeguards sensitive data and user identities. Regularly reviewing the Attack Protection Log Events allows you to identify patterns, assess risks, and take timely actions to mitigate potential threats. Our dedicated support team is available to assist you in navigating any challenges or implementing additional security features tailored to your organization's needs. Together, let's ensure the integrity and reliability of your ***AuNEX0 IAM*** experience, empowering you to manage identities with confidence and peace of mind.