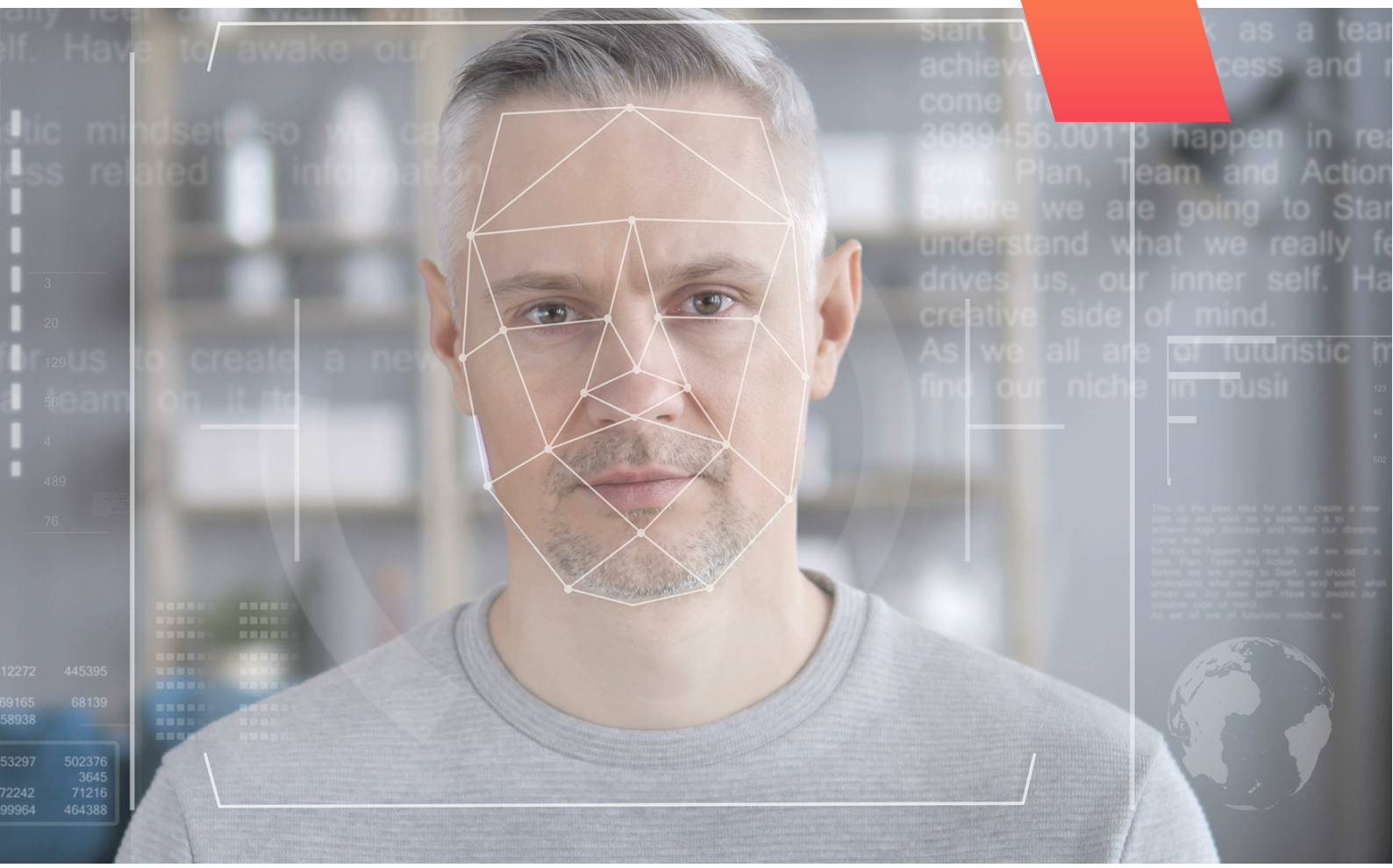
WHITEPAPER

Identity and Access Management - The Key to the Treasure Trove

Identity Access Management (IAM) is the basic building block for Authentication, Authorization, and Auditing/Accounting (AAA).

With an IAM framework in place, Information Technology (IT) managers can control user access to critical information within their organizations.



"No man is an island entire of itself; every man
is a piece of the continent, a part of the main…"
MEDITATION XVII
Devotions upon Emergent Occasions
John Donne[i]

We are all connected, hence the need for Identity and Access Management (IAM).

Identity And Access Management (IAM) is a framework of business policies, processes, and technologies that facilitates the management of digital identities.

IAM is the security discipline that makes it possible for the right entities (people or things) to use the right resources (applications or data) when they need to, without interference, using the devices they want to use. In other words, IAM is the basic building block for Authentication, Authorization, and Auditing/Accounting (AAA).

Stop! Who goes there?

With digital transformation reaching a crescendo, IAM needs to cover the employees, contractors, business partners, remote and mobile users, and customers in its ambit. Identities are also assigned to the Internet of Things (IoT) devices, robots, and pieces of code such as APIs or microservices. Multi-cloud hybrid IT environments and Software-as-a-Service (SaaS) solutions also require IAM.

IAM implementation

With an IAM framework in place, Information Technology (IT) managers can control user access to critical information within their organizations. Systems used for IAM include Single Sign-On Systems (SSO), Two-Factor Authentication (TFA – like Username and Password), Multi-factor Authentication (MFA – like OTP), and Privileged Access Management (PAM). These technologies also provide the ability to securely store identity and profile data as well as data governance functions to ensure that only data that is necessary and relevant is being shared.

Key challenges

The COVID-19 pandemic has suddenly created an explosive demand for remote work at an unprecedented scale. A hybrid work environment is increasingly the norm for a large part of the workforce in many enterprises. This work environment makes it imperative to secure the enterprise assets with a range of technologies including Desktop-as-a-Service (DaaS), Virtual Desktop Infrastructure (VDI), Zero Trust Network Architecture (ZTNA), and Cloud Access Security Broker (CASB). Secure remote access to on-premises and cloud applications requires IAM controls that these tools cannot natively provide.

Bow Out, O powerless password...

Although being ubiquitous password-based authentication has become the weakest chink in the armor. In case of account takeover (ATO) and other digital-identity risks, they have merely become a log entry, without any substantive mitigation. As per Gartner, compromised passwords account for more than 60% of breaches due to hacking.[ii]

Identity and access management (IAM) consumers while seeking to eliminate passwords, are often uncertain of what a passwordless authentication should look like.

Moreover, IAM consumers are often hesitant of investing in technologies that are short-lived and might entail a lot of effort and gestation period or by the lack of a universal acceptance.

The journey towards a passwordless future

As per Gartner: By 2025, more than 50% of the workforce and more than 20% of customer authentication transactions will be passwordless, up from less than 10% today.[1]

Multi-factor authentication can be achieved by adding a kind of token to the legacy password. While this can significantly reduce risks, the password remains a weak link, putting a significant burden on the additional factors like OTP, Security Questions, Biometrics, etc. With or without additional factors, passwords can be a significant source of friction and frustration for users and administrators.

A passwordless authentication method uses any credential or combination of credentials and signals that isn't or doesn't include a password.

How to achieve a frictionless authentication experience

A journey toward passwordless authentication has four steps. Let's look at them.

Start with MFA implementation

For MFA, each additional factor is intended to increase the assurance that an entity involved in some kind of communication or requesting access to a system is who - or what - it says it is.

MFA works by combining two or more factors from the categories mentioned below:

- **Time**: The ubiquity of smartphones and the presence of Global Positioning System tracking provides credible confirmation of the login location.
- **Location**: It is used to prove a person's identity by detecting presence at a specific time of day and granting access to a certain system or location. For example, bank customers cannot physically use their ATM cards in India and then in China 15 minutes later.
- **Something you know, or the knowledge factor**: This category requires the user to answer a personal security question and generally includes passwords, four-digit personal identification numbers (PINs), and one-time passwords (OTPs).
- **Something you have, or the possession factor**: Users must possess something specific to log in, such as a badge, token, key fob, or phone subscriber identity

module (SIM) card, or a phone call sent to a user. For mobile authentication, a smartphone often provides the possession factor in conjunction with an OTP app.

- **Something you are, or the inherence factor**: Any biological traits the user has that are confirmed for login. Inherence factors include the following Biometric verification methods:
    - Retina Or Iris Scan
    - Fingerprint Scan
    - Voice Authentication
    - Hand Geometry
    - Digital Signature Scanners
    - Facial Recognition
    - Earlobe Geometry

To start on the path to "passwordless", organizations should first implement two-factor authentication, which uses passwords as a starting point and a non-password authentication method as a second factor.

From there, make the move to MFA. This helps users get used to the passwordless experience before making a full transition. It teaches employees how biometrics, smart cards, and other passwordless methods work, in turn reducing friction during future full-passwordless onboarding processes.

Trust the Zero Trust

The push for passwordless makes zero-trust architecture adoption a logical first step for companies. In contrast to the traditional "castle-and-moat" model, where all users are trusted once past the network perimeter, in the zero-trust model, no user or device is trusted just because they have been allowed onto the network. Instead, strict user and device authentication and authorization is required throughout the network to verify the identity and access rights of the person or entity requesting access.

Zero-trust security is all about granular authentication and contextual authorization for every request, whether on-premises, in the cloud, or hybrid, with runtime evaluation of user, device, app, and data attributes against access control policies. It is the embodiment of the principle of least privilege by limiting access to only those who require it to do their work, thereby reducing the opportunity for hackers to move laterally through networks.

Zero trust also helps companies better accommodate identity management for employees accessing corporate resources remotely. It can provide continuous authentication and help lower dependence on knowledge-based authentication factors that are easily spoofed.

Add continuous authentication

Continuous authentication is a method of verification aimed at providing identity confirmation and cybersecurity protection by constantly measuring the probability that individual users are who they claim to be. Continuous authentication validates the user not just once but non-stop throughout an entire session. Focused on furnishing smart, secure identity verification without interrupting the workflow, continuous authentication is implemented using machine learning (ML) and a variety of factors including behavioral patterns and biometrics.

Bring in behavioral biometrics

Another identification measure helping enterprises embrace continuous authentication and passwordless is behavioral biometrics. Using factors such as location, gait, and device use, behavioral metrics distinguish between legitimate users and impersonators using a risk score. If an activity raises the risk score beyond a certain threshold, the user is prompted for additional authentication factors, such as a one-time password or facial recognition.

SSO – the unifying thread

Single sign-on (SSO) is a session and user authentication service. It permits a user to use one set of login credentials - for example, a name and password - to access multiple applications. An SSO can be used by enterprises, smaller organizations, and individuals to ease the management of various usernames and passwords.1

Single sign-on is a federated identity management (FIM) arrangement, and the use of such a system is sometimes called an identity federation. SSO services depend on protocols like Kerberos, and Security Assertion Markup Language (SAML).

Accops MFA solution suite

Accops HyID

Accops HyID is an identity and access management (IAM) solution aimed to safeguard critical business applications and data from internal and external threats. HyID provides enterprises with strong control over endpoints, enabling contextual access, device entry control, and a flexible policy framework.

The out-of-the-box MFA is compatible with all modern and legacy apps, cloud and on-prem apps. It enables strong authentication based on OTP delivered via SMS, email, and app, biometrics, and device hardware ID & PKI.

The Single sign-on (SSO) feature provides better security and convenience.
Using HyID, enterprises can monitor the security posture of the endpoints, including BYOD devices, and grant or deny access based on real-time risk assessment. With HyID in place, the system can generate alerts if access to any corporate application by a user breaches the set risk thresholds.

HyID provides actionable intelligence, enabling organizations to detect and prevent identity thefts and misuse of privilege rights. Detailed audit logs on who accessed what, when, and how, enable compliance with regulatory norms.

Accops BioAuth

Accops BioAuth is a biometric authentication server providing fingerprint and face authentication solutions. BioAuth can be used to quickly enable biometric-based multi-factor authentication to any corporate application or PC, or laptop.

Organizations can choose between fingerprint and facial-based authentication or bring their fingerprint scanners and use BioAuth to manage the biometric data capturing, enrolment, identification, and authentication of users. BioAuth's flexible workflow enables the maker-checker process for user onboarding possible in any

complex organizational structure. BioAuth provides support for multiple fingerprint readers as well as Microsoft Windows WinBIO.

BioAuth integrates out of the box with **Accops HySecure** (Secure Remote Access solution) to enable strong MFA to remote users. When integrated with Accops HyID,

BioAuth can be used for any corporate application that supports Microsoft Active Directory or SAML protocol for authentication.

Conclusion

An IAM solution stands between users and critical enterprise assets and hence is a critical component of any enterprise security program. It helps protect the organization against insider threats originating from compromised user credentials and easily cracked passwords. These weak links are the most common network entry points for criminal hackers who want to plant ransomware or steal data.

Done well, IAM helps ensure business productivity and frictionless functioning of digital systems. Employees can work seamlessly no matter where they are, while centralized management makes sure, they only access the specific resources they need for their jobs, simultaneously opening systems to customers, contractors and suppliers can increase efficiency and lower costs.

---

[i] John Donne
[ii] Gartner - Take 3 Steps Toward Passwordless Authentication

accops

India
3rd Floor, Fiesta, Old Mumbai Road, near Renault Showroom, Baner,
Pune, Maharashtra, 411069
Email: contact@accops.com
Website: accops.com

About Accops

Accops enables secure and instant remote access to business applications from any device and network, ensuring compliant enterprise mobility for business users while keeping governance with the organization.

©2025 Accops Systems, Inc. All rights reserved