HOW COULD AN

IDENTITY & ACCESS GOVERNANCE SOLUTION

PREVENT A CYBER ATTACK?

An enterprise needs to implement Identity and Access Governance (IAG) across its IT environment to avoid or minimize the impact of a cyber-attack. In this infographic, we explore six processes on how IAG can prevent a business from potential cyber-attack.

Organization wide **strong access control**

The IAG solution consumes all the identities from the directories/ID stores- located in the cloud or on-premises. If any changes occur, the solution in-sync consolidates the identity types in real-time, without falling back in status updates that cybercriminals could pounce on.

Automates the Process of **Access Privilege**

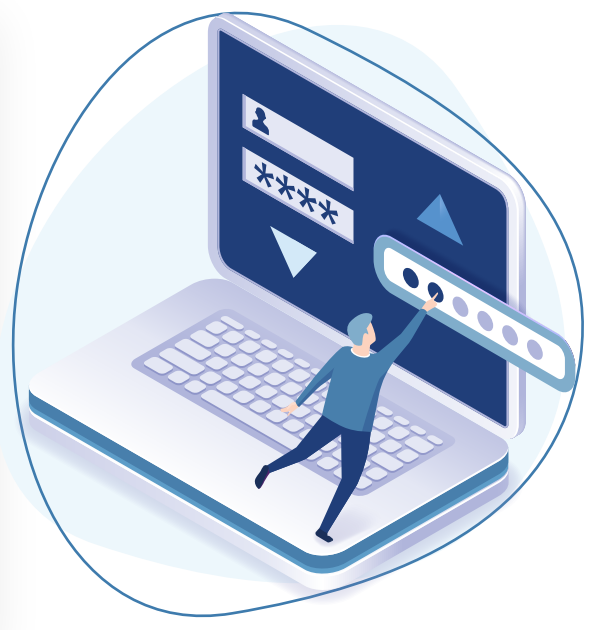
For every new hire, the IAG solution provides features to assign all the privileges based on specific roles and business policies with work-flow automation. Besides, if an employee leaves or gets terminated from the organization, the solution ensures all the access privileges are revoked automatically.

Provides Controls Over **Privileged Accounts**

Cyber attackers cause the most damage to an organization by breaching its IT environment through compromised privileged accounts. The privileged accounts are often used by cyber-criminals to gain access to the most critical data or information systems of the organization. IAG enables you implement robust controls & frequent access attestations that helps mitigate access risks.

Ensures Strong **Password Policy**

A weak password could be easily hacked or obtained by cybercriminals using various social engineering or phishing techniques. The platform allows you to define and enforce strong password policies so end users don't set passwords that can be easily cracked by brute-force attacks.



Enables **Multi-Factor Authentication (MFA)**

Hackers could easily intrude in your IT systems if the password is the only security mechanism. Multi-Factor Authentication (MFA) provides an extra layer of security through smart cards, One Time Password (OTP), and security tokens. MFA enhances your security infrastructure postures and makes cyber attackers' access to your systems more difficult.

Clean-up **unused or orphan accounts**

The IAG solution provides the ability to generate periodic analytics and reporting to identify orphan or unused accounts in the system. The solution makes sure accounts have owners who are accountable. Along with this, it helps get rid of unused/inactive accounts and mitigate their accesses and privileges to your data, applications, and systems.