SafePaaS™

The Definite Guide to

Modern Identity and Access Management – IGA, IAM, and PAM

Misuse of user identity is the root cause of most cybersecurity incidents. Threats can manifest as a bad actor impersonating an authorized system user, creating fake user accounts, or an insider exploiting their access.

Identity has evolved beyond a tool and is now a modern strategic framework to secure digital assets and protect data. Identity protects resources, supports digital transformation and risk initiatives, and strengthens data protection policies using security standards.

Identity security also enables organizations to centrally manage their expanding perimeter, including mobile and remote users and on-premises, multi-cloud, and hybrid infrastructure. Consequently, an identity platform is necessary to manage accounts across the organization's applications.

According to the 2021 Identity and Access Management Report, the "increasing importance of managing access is part of an organization's overall risk management and security posture in the new normal of hybrid work locations." Key findings of the report include:

- **87%** view IAM as very to extremely important to their risk management and security posture.
- **77%** have at least a few users with more access privileges than required for their jobs.
- **76%** of organizations saw a reduction in unauthorized access from using an IAM solution. .

The three pillars of identity

User identity is the most significant element in an organization's security framework. Identity security is designed to provide users with secure, frictionless access to resources. In the context of identity, a "user" can represent a broad range of people and things, including privileged users, employees, contractors, consumers, servers, service accounts, application programming interfaces (APIs), and the Internet of Things (IoT) devices.

Modern identity and access management is composed of three critical components:

- **Access Management (AM)**,
- **Identity Governance Administration (IGA)**, and
- **Privileged Access Management (PAM)**

Automation and interoperability of these components are essential to ensure all applications, systems, APIs, policies, and processes work smoothly.

What is access management (AM)?

AM strengthens security and reduces risk by controlling access to on-premises and cloud applications and infrastructure. Most access management solutions grant access privileges through:

- **Identification,**
- **Authentication,** and
- **Authorization,**

Access management ensures users have authorized access to specific resources appropriate for their job function.

SafePaaS™

What is identity governance and administration (IGA)?

IGA is a policy framework enabling organizations to effectively mitigate identity-related access risks. IGA solutions automate creating, managing, and certifying user accounts, roles, and privileges for users in an organization.

IGA solutions facilitate user provisioning, policy management, access governance, and access certification. Considered to be part of IAM, IGA offers organizations increased visibility into users' identities and access privileges. Streamlining these processes allows organizations to better control who has access to what assets and when.

What is Privileged Access Management (PAM)?

PAM is a critical security control that enables organizations to streamline managing and monitoring privileged access across systems, applications, and infrastructure.

Managing PAM is challenging for many organizations because administrator accounts have elevated privileges to sensitive data, applications, and transactions, while many PAM solutions lack the capability to record user activity.

Of the three pillars, PAM is the most limited in scope. AM and IGA focus on a broader range of activities that govern and manage user access to resources, systems, and applications across the organization. While PAM defines and controls access for privileged users and accounts. The three types of privileged accounts are:

- **Administrator Accounts** are used to modify files and configurations and administer operating system services.
- **System Accounts** have no restrictions in accessing services or data on the organization's server and are a prime target for bad actors.
- **Service Accounts** can access data, resources, and configurations to run processes and applications through automated and typically unguarded tasks. Service accounts are also set up to facilitate API services in the cloud.

SafePaaS™

Unified IGA, AM, and PAM

Integrating IGA, AM, and PAM creates a central hub of policy, governance, and enforcement of identity security. With an integrated policy-based approach, a privileged access request can be managed within the organization's IGA policies. Privileged access requests and approvals are part of the access control chain of authority, making privileged access more easily auditable.

Many enterprises use end-point solutions to handle their identity-related challenges. However, those solutions do not integrate with other applications, servers, and databases. With identity orchestration, organizations can automate the management of their legacy IAM and ITSM systems and eliminate silos.

Benefits of unified IGA, AM, and PAM

- A single hub for provisioning and managing access
- Enforcement of identity governance policies for privileged access sessions
- Simplified auditing of user access, including segregation of duties violations and other access compliance policies
- Streamlined process of onboarding and off-boarding privileges
- Reduced costs by consolidating existing point solutions with a single-platform solution

SafePaaS™

How you can benefit from unified IGA, AM, and PAM

COMPLETE ACCESS VISIBILITY

Complete user access visibility is a major challenge for many organizations, from provisioning and certification to de-provisioning access. The inability to view cross-application user access data creates weaknesses and inefficiencies caused by overlapping and duplicated lifecycle management processes.

Organizations with complex enterprise systems need life cycle management to **control access for employees, contractors, and third parties**. Changes to work duties or departures from the organization require quick updates to access privileges that comply with governance policies ensuring users only have access to what they need and removing excessive access.

Policy-based access management also improves user productivity while preventing unauthorized users from accessing business-critical systems by providing consistent, automated policy controls with fine-grained visibility.

For example, you can:

- Achieve visibility into fine-grained access and privileged accounts and help stop over-entitled users
- Detect access policy violations by automating access certification reviews and approvals of privilege updates
- Streamline and speed up provisioning and de-provisioning by modifying access based on user roles and lifecycle changes
- Control and enforce third-party security policies
- Govern privileged accounts that provide a backdoor for bad actors who have retained access

SafePaaS™

EASY POLICY CREATION AND ENFORCEMENT

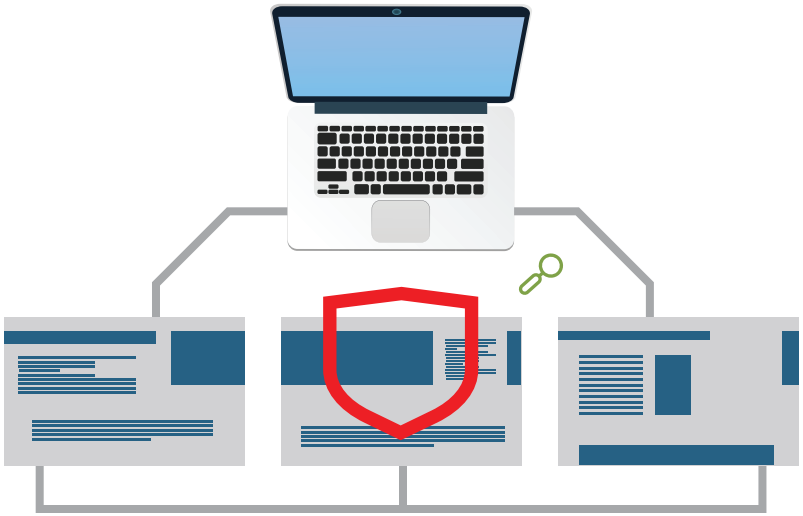
Policies are critical to every organization. They communicate how your organization governs access and data and how you mitigate any associated risks.

A critical element of governance is managing and controlling the current and future use of digital resources. Policies establish the requirements for how the organization handles specific operations, including suppliers, partners, and other stakeholders.

Effective policy management can prevent toxic combinations of access within your organization that can lead to fraud and abuse. Another benefit of implementing proper policy management is to reduce the risk of error. For example, if you only have one person responsible for defining and assigning user permissions, that person could define super-user permissions to themselves and cause significant damage. Having multiple people involved in the permissions process helps avoid insider threats.

RECORDED SNAPSHOT SECURITY MODEL

Evaluating user access is critical to minimize risk and comply with the organization's access policies. Understanding all the roles, privileges, and other security attributes that grant user access to perform process activities is necessary. Any violations detected during this evaluation step require the security administrator to make the necessary remediation recommendations and address the known incidents. For example, the Oracle ERP Cloud security model is flexible, but its design is complex, so it's essential to design and build security in the implementation phase to ensure the effective segregation of duties.



SafePaaS™

EXECUTE THE PRINCIPLE OF LEAST PRIVILEGE

The principle of least privilege (PoLP) refers to the concept that all user access should be given as few privileges as possible and run applications with as few privileges as possible. PoLP also controls access creep or users who accumulate access privileges.

AUTOMATED USER LIFECYCLE MANAGEMENT OF PRIVILEGED ACCESS

Automated identity lifecycle management of privileged access increases user productivity and organizational security. The primary use cases for privileged access management are controlling credential theft and regulatory and policy compliance.

Credential theft is when log in information is stolen to obtain access to a user's account. Once logged in, the threat actor can access data, install malware, and even acquire access to other systems like your ERP or business solution. PAM mitigates the risk of threat actors gaining access by providing timed access for all identities and accounts.

PAM also facilitates compliance by providing supporting documentation of all privileged user activity, such as who accessed what data and why.

Misusing privileged access is a cybersecurity threat that can cause severe damage to any company. PAM offers features to help you mitigate damaging risks.

- Monitor and record privileged sessions to support audits and compliance
- Provide timed access to critical resources
- Analyze unusual privileged activity
- Automated attestation of privileged access

SafePaaS™

THIRD-PARTY SECURITY

Controlling an organization's sensitive data is crucial, but ensuring third parties follow your security policies is challenging. Giving privileged account access to third parties is a risk that can leave you vulnerable. Maintaining visibility over your third parties and their superuser accounts to ensure that their access level isn't being misused or abused is critical to ensure you're safeguarded.

Security and compliance consume time, money, and resources from companies and can often hinder the ability to achieve more ambitious operations goals. Security and compliance solutions that scale rapidly, improve productivity, and integrate with new technologies for cloud, hybrid, and on-premise environments will become necessary as companies evolve. SafePaaS makes identity access management effortless for any organization

To learn more about how SafePaaS can help, please, **contact us**.

3300, Dallas Parkway, Suite 200, Plano, Texas, 75093 USA

SafePaaS™