International Journal of Multidisciplinary Research and Growth Evaluation.

Identity Access Management, Identity Governance Administration, Privileged Access Management differences, tools and applications

Seema Kalwani
Security Engineer, IL, USA

* Corresponding Author: **Seema Kalwani**

Article Info

ISSN (online): 2582-7138
Volume: 06
Issue: 02
March-April 2025
Received: 05-03-2025
Accepted: 01-04-2025
Page No: 1832-1839

Abstract
The article provides an overview, definitions, functioning, importance, differences, technology and tools for Identity Access Management (IAM), Identity Governance and Administration (IGA), Privileged Access Management (PAM) covering the benefits, workflows of the tools used to implement identity security landscape in enterprises.

DOI: https://doi.org/10.54660/.IJMRGE.2025.6.2.1832-1839

Keywords: PAM, CyberArk, Identity and Access Management, IAM, IGA, Privileged Access Management, Identity and Governance Administration, Omada, Symantec, OIDC, SCIM, SAML

Introduction

I. Introduction to identity security landscape

The identity security landscape has transformed considerably within the last two decades. And for good reason. Mitigating identity-related access risks has become essential as companies face threats every day, from virtually everywhere.

The focus on managing the access of people, digital identities, and privileged accounts has increased significantly to address risks, and has put Identity and Access Management (IAM), Identity Governance and Administration (IGA), and Privileged Access Management (PAM) in the forefront of identity programs within companies today.

But what really is the difference between these three interrelated areas and how can organizations leverage them within their own identity strategies and programs? This article will examine the relationship between IAM, IGA, and PAM, and provide practical insights for leveraging them appropriately in your organization.

II. Identity and Access Management (IAM)

A. Introduction

Identity and Access Management is an essential part of overall IT security that manages digital identities and user access to data, systems, and resources within an organization. IAM security includes the policies, programs, and technologies that reduce identity-related access risks within a business.

Gartner defines IAM simply as 'the discipline that enables the right individuals to access the right resources at the right times for the right reasons.' As a critical security function, IAM enables companies to not just respond to changes in the business, but also become more proactive in anticipating identity-related access risks that result from the dynamic business environment.

According to the 2020 Identity and Access Management Report, 90 percent of organizations confirm that IAM is very to extremely important as part of their cybersecurity and risk management posture. This confirmation of IAM as a strategic imperative means it should be viewed from a cross-functional perspective of stakeholders—from business leaders, IT and security teams, customers, auditors, employees, contractors and non-employees, vendors and partners.

A solid approach to IAM enables organizations to mitigate risks, improve compliance, and increase efficiencies across the enterprise. That's why overseeing appropriate access through the right IAM framework goes a long way towards bolstering risk

management within the organization and closing the gap on overall IAM risk.

B. IAM Functioning

There are two parts to granting secure access to an organization's resources: Identity management and access management.

1. Identity management

Identity management checks a login attempt against an identity management database, which is an ongoing record of everyone who should have access. This information must be constantly updated as people join or leave the organization, their roles and projects change, and the organization's scope evolves.

Examples of the kind of information that's stored in an identity management database include employee names, job titles, managers, direct reports, mobile phone numbers, and personal email addresses. Matching someone's login information like their username and password with their identity in the database is called authentication.

For added security, many organizations require users to verify their identities with something called multifactor authentication (MFA). Also known as two-way verification or two-factor authentication (2FA), MFA is more secure than using a username and password alone. It adds a step to the login process where the user must verify their identity with an alternate verification method. These verification methods can include mobile phone numbers and personal email addresses. The IAM system usually sends a one-time code to the alternate verification method, which the user must enter into the login portal within a set time period.

2. Access Managment

Access management is the second half of IAM. After the IAM system has verified that the person or thing that's attempting to access a resource matches their identity, access management keeps track of which resources the person or thing has permission to access. Most organizations grant varying levels of access to resources and data and these levels are determined by factors like job title, tenure, security clearance, and project.

Granting the correct level of access after a user's identity is authenticated is called authorization. The goal of IAM systems is to make sure that authentication and authorization happen correctly and securely at every access attempt.

C. The importance of IAM for organizations

1. One reason IAM is an important part of cybersecurity is that it helps an organization's IT department strike the right balance between keeping important data and resources inaccessible to most but still accessible to some. IAM makes it possible to set controls that grant secure access to employees and devices while making it difficult or impossible for outsiders to get through.
2. Another reason that IAM is important is that cybercriminals are evolving their methods daily. Sophisticated attacks like phishing emails are one of the most common sources of hacking and data breaches and they target users with existing access. Without IAM, it's difficult to manage who and what has access to an organization's systems. Breaches and attacks can run rampant because not only is it difficult to see who has access, it's also difficult to revoke access from a compromised user.

While perfect protection unfortunately doesn't exist, IAM solutions are an excellent way to prevent and minimize the impact of attacks. Instead of restricting everyone's access in the event of a breach, many IAM systems are AI-enabled and capable of detecting and stopping attacks before they become bigger problems.

D. IAM technologies and tools

IAM solutions integrate with a variety of technologies and tools to help make secure authentication and authorization possible on an enterprise scale:

1. Security Assertion Markup Language (SAML) – SAML is what makes SSO possible. After a user has been successfully authenticated, SAML notifies other applications that the user is a verified entity. The reason SAML is important is that it works across different operating systems and machines, which makes it possible to grant secure access in a variety of contexts.
2. OpenID Connect (OIDC) – OIDC adds an identity aspect to 0Auth 2.0, which is a framework for authorization. It sends tokens containing information about the user between the identity provider and service provider. These tokens can be encrypted and contain information about the user such as their name, email address, birthday, or photo. The tokens are easy for services and apps to use, which makes OIDC helpful for authenticating mobile games, social media, and app users.
3. System for Cross-Domain Identity Management (SCIM) – SCIM helps organizations manage user identities in a standardized way that works across multiple apps and solutions (providers). Providers have different requirements for user identity information, and SCIM makes it possible to create an identity for a user in an IAM tool that integrates with the provider so that the user has access without creating a separate account.

III. Identity Governance and Administration (IGA)

A. Introduction

IGA is both a policy framework and set of security solutions that enable organizations to more effectively mitigate identity-related access risks within their business. IGA automates the creation, management, and certification of user accounts, roles, and access rights for individual users in an organization. This means companies can streamline user provisioning, password management, policy management, access governance, and access reviews within their business.

Another definition of identity governance, is the 'policy-based centralized orchestration of user identity management and access control,' indicating the function 'helps support enterprise IT security and regulatory compliance.' Put into simpler terms, IGA means leveraging the most intelligent and efficient path to mitigating identity risk in your business.

Considered part of Identity and Access Management, Identity Governance and Administration offers organizations increased visibility into the identities and access privileges of users, so they can better manage who has access to what systems, and when. Identity governance empowers organizations to do more with less, enhance their security posture, and meet increasing auditor demands, while also scaling for growth.

B. IGA Functioning

Identity Governance and Administration provides automation capabilities for creating and managing user accounts, roles, and access rights for individual users within organizations. With IGA, organizations can easily leverage a more secure, strategic, and streamlined approach for provisioning and deprovisioning, user lifecycle management, compliance and governance, password management, access certifications, and risk insight. Identity governance also enables companies to:

- Improve organizational security and reduce identity-related risk
- Leverage role-based access for intelligent, visible role management
- Streamline certification processes to comply with increasing auditor demands
- Ensure compliance with government regulations and industry standards
- Boost operational efficiencies to empower the business to do more with less

C. IGA versus IAM

IGA differs from IAM in that it allows organizations to not only define and enforce IAM policy, but also connect IAM functions to meet audit and compliance requirements. This means Identity Governance and Administration has the distinct purpose to ensure IAM policies are connected and enforced.

IV. Omada identity cloud as IGA solution features and benefits

A. Informed decisions with role insights and identity analytics

Make informed decisions about user access with data-driven insights. Omada Identity Cloud leverages advanced analytics and machine learning to provide a deep understanding of user behavior and access patterns, enabling you to optimize roles, identify potential risks, and streamline compliance efforts.

1. Benefits

- Identity Analytics offers a unified view of user access across the organization, simplifying compliance reporting by transforming raw data into actionable insights.
- Automate role discovery based on user behavior with Role Insights, optimizing access and reducing security risks.
- Easily demonstrate compliance with regulations, minimizing the risk of audits and fines.

Fig1: Role insights from Omada from OmadaIdentity website.

B. Identity lifecycle management

Omada Identity Cloud provides a comprehensive solution for identity lifecycle management, covering joiner, mover, and leaver processes for all identity types. We provide a more efficient and secure identity management process by automating policy and role management and offering unified provisioning across IT systems.

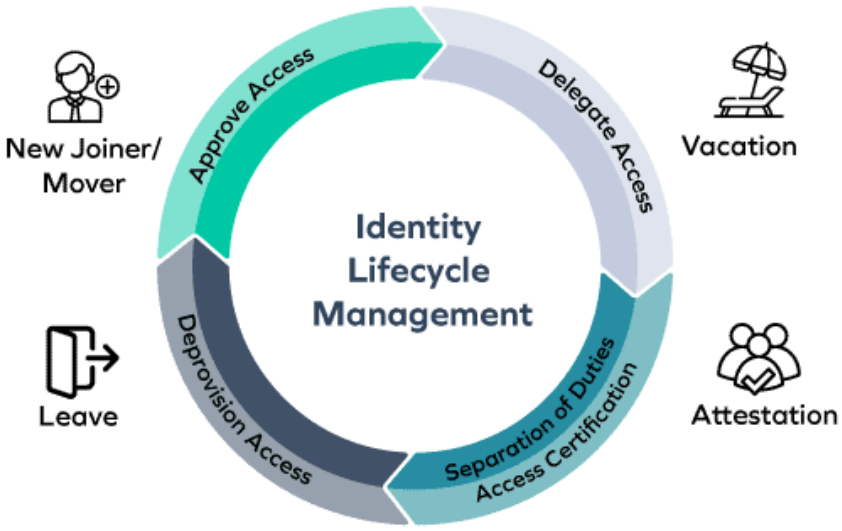

FIg 2: Identity Life Cycle Management from Omada Identity site.

1. Benefits

- Effortlessly and automatically control all identity types as they join, move, and leave the enterprise, removing the need for manual, error-prone processes
- Streamline compliance efforts, reduce the risk of human error, and improve operational efficiency by ensuring consistent and proactive management of access policies and roles across the organization
- Centralize user access management and simplify administrative tasks for more efficient and effective IT operations

C. Configurable workflows

Omada Identity Cloud's workflow engine provides you with highly adaptable process flows tailored to your unique business needs, supporting manual, triggered, or scheduled workflows. We provide pre-configured email integration and prompts, facilitating seamless communication and ensuring efficient task management within your organization.

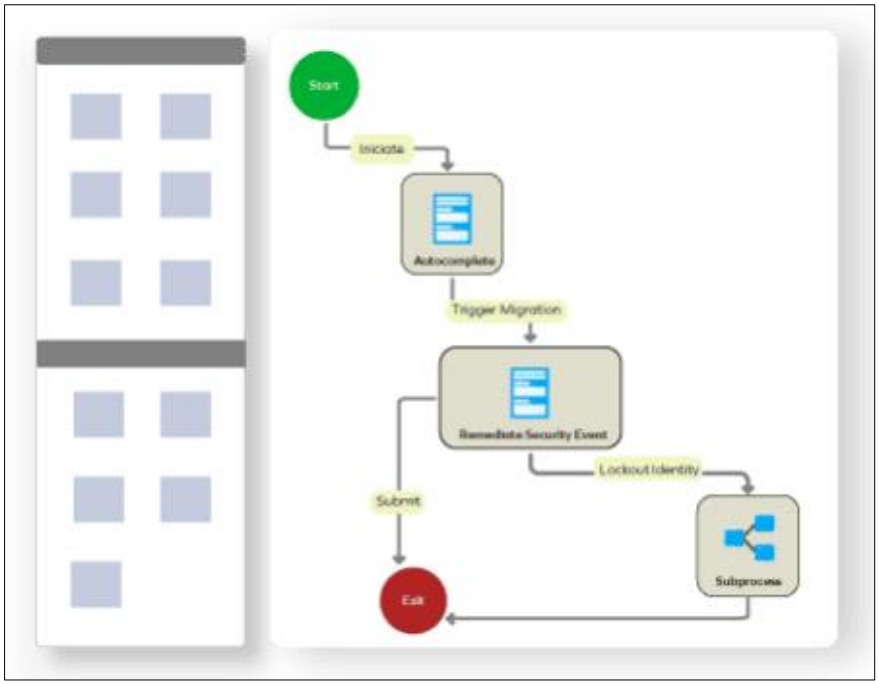

Fig 3: Configurable Workflows from Omada Identity Site

1. Benefits

- Streamline organizational processes, optimize task management, and adapt to evolving business needs
- Providing you with the flexibility to choose the most suitable workflow approach for your specific requirements
- Facilitate efficient communication, timely notifications, and seamless collaboration within each workflow

D. Certification

Omada Identity Cloud provides configurable certification surveys for user entitlement, account, and permission reviews. These certifications can be event-triggered or scheduled for periodic re-certification. We also offer central

monitoring for streamlined oversight, bolstering security and compliance.

D. Benefits

- Tailor the certification process to your specific business and compliance requirements
- Maintain continuous oversight to ensure that certifications comply with evolving security and compliance standards
- Streamline administration efforts and increase efficiency through effective management and reporting

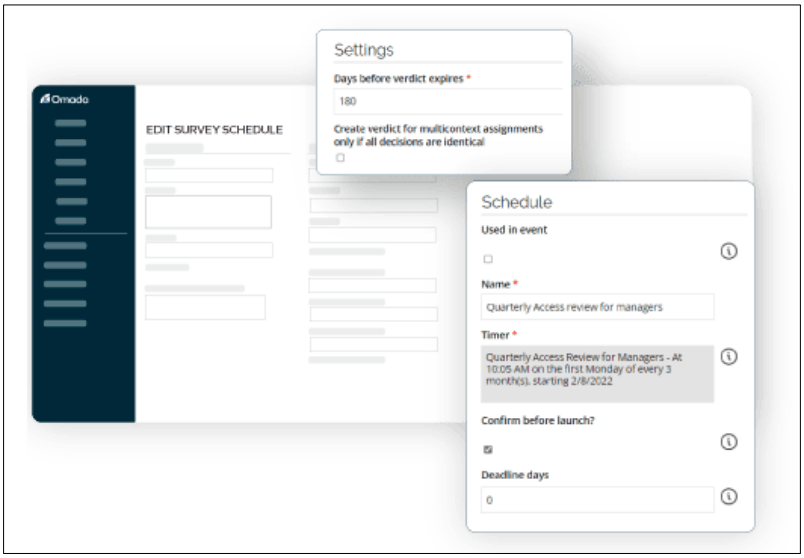

FIg 4: Certification screen from Omada Identity Site.

E. Compliance and Risk

Omada Identity Cloud provides strong compliance and risk mitigation with comprehensive reporting and audit trails, user-friendly dashboards, and baked-in risk scoring that supports proactive risk management within approval workflows and access reviews. With the Omada Compliance Workbench, you have full visibility into the compliance level of each onboarded application and system. The Workbench also empowers you to take immediate remedial actions, ensuring that any issues are promptly addressed.

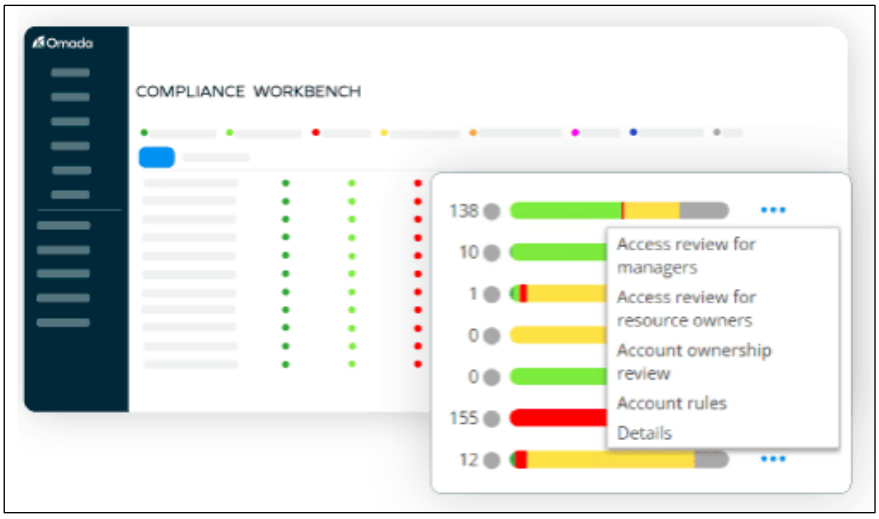

Fig 5: Compliance and Risk screen from Omada Identity Site.

1. Benefits

- Clear insights into your compliance status and risk exposure
- Optimize managing all compliance-related activities and reporting
- Proactively identify and mitigate potential security and compliance risks

V. Privileged Access Management (PAM)

A. Introduction

PAM is considered a critical security control that enables organizations to simplify how they define, monitor, and manage privileged access across their IT systems, applications, and infrastructure.

Because administrator accounts have elevated privileges that can access valuable data and execute applications or transactions—often with little or no tracking control—it can be very difficult to manage privileged accounts. PAM solutions centralize management of administrator profiles and ensure least privilege access is enforced to give users only the access they need.

Of each of the three areas discussed here, PAM is the most

narrowly defined, but has the significant responsibility for mitigating identity-related access risks related to privileged access. While IAM and IGA focus on wider levels of user access for resources, systems, and applications across the organization, PAM primarily defines and controls access for privileged users.

B. Privileged Accounts

Privileged accounts are typically shared accounts that inherently possess elevated access to data or services. In more vivid terms, these accounts are considered elevated accounts within your IT environment that hold the 'keys to the kingdom.' Examples of elevated privileges include the ability to change system configuration, to install or remove software, or to add, remove or modify user accounts. Elevated privileges can also just simply be access to sensitive data. Below are three specific types of privileged accounts:

1. Root/Administrator Accounts: These accounts possess full authority to systems and have no restriction for accessing services or data residing on a server. They are considered the most valuable targets for threat actors.
2. System Accounts: These accounts are used for running operating system services and can modify the relevant files and configurations. They are typically provisioned with the operating system.
3. Service/Application Accounts: These accounts are used for running processes and applications through automated, often unattended tasks. They frequently own or have access to data, resources, or configurations not available to non-privileged users.

Each organization should determine what is classified as privileged data, where it is, and who has access to it. Control of privileged accounts is a major factor in compliance across regulations in every industry. Because of their elevated access, privileged accounts have more significant risks than non-privileged accounts and have more potential for exploit or abuse. Privileged accounts, which can number in the hundreds in some enterprises, are frequently not tied to specific individuals, so the accounts can be used to do virtually anything, with little or no possibility of detection.

C. Privileged Account and Session Management (PASM) and Privilege Elevation and Delegation Management (PEDM)

Both PASM and PEDM use the principle of least privilege, which mandates that users only have the access necessary to their job functions, but have different mechanisms in how the target account is protected and accessed.

PASM solutions are often referred to as password vaulting. Privileged account credentials are securely created and distributed exclusively by the solution. When users need access to a specific server, they request access from the vault, and are given a temporary account with full administrative privileges. This account is only valid for a single session. Additionally, the session activity is monitored and recorded.

Leading PEDM solutions distribute access privilege based on job roles. Instead of using temporary privileged accounts, PEDM tools assign permanent privilege to standard accounts. PEDM tools define who can have access to each part of a system as well as what they can do with that access. This approach scales much better, centralizes management, and enhances overall security.

VI. Symantec Pam

Protecting privileged access has moved beyond the vault and enterprises require a platform that can scale to secure an exponential number of accounts and credentials with elevated access and is flexible enough to cover a wide variety of use cases. A brief of the features that Symantec PAM provided

1. Credential vault: Store privileged credentials in an encrypted vault and only grant access after users have been positively identified.
2. Zero Trust Access: Implement zero trust approach that denies all access by default and only grants access through explicit policies.
3. Threat Analytics: Monitor privileged user activities to assess risk and trigger automatic mitigation actions when unusual behavior is detected.
4. Session Recording: Capture a video of all privileged user actions to improve accountability and provide forensic evidence of malicious activity.
5. Fine-Grained Access: Enforce fine-grained access controls over super user accounts to support secure task delegation and compromised accounts.
6. Secrets Management: Enable applications and scripts to retrieve secrets from an encrypted vault rather than have these credentials hard-coded.

FIg 6: Privileged Access Manager Solution taken from Broadcom training docs.

A. Policy Enforcement
Policy enforcement compartmentalizes high-risk users using integrated Java applets with a reverse port-tunneling access technology that provides segregation of critical IT infrastructure components and separation of duties that easily meets compliance requirements. Users are contained within these compartments through the CA Technologies Leap Frog Prevention™ technology, which employs a whitelist/blacklist approach, blocking users from leaving authorized areas at the socket level.

B. User activity monitoring
User activity monitoring watches user activity with real-time alerts for attempted policy violations. Administrators are notified immediately when an access violation has been attempted, detected, and prevented. Access might be terminated when a user attempts to access an unauthorized system or device.

C. User event recording
User event recording provides centralized tracking of all activities and events using session recording and playback capabilities. An administrator can have complete visibility into user activities in CLI sessions. You can configure event recording that is based on individual user profiles or individual back-end devices. All command line activity is monitored, recorded, and archived for audit and compliance purposes.

D. Centralized Reporting
Centralized reporting provides comprehensive, customized audit and compliance reports for any user-initiated events. The reports can include usage data and attempted security violations. You can also run automated reports that are focused on the compliance of individual users. You can configure the automated reports to run at predetermined intervals and then distribute the reports using email.

E. Privileged Access Management Server Control (PAM SC)
The Server Control module makes the PAM Server the central management server for all Server Control functions. The Server Control module replaces the Enterprise Management Server in the standalone PIM and PAM SC products. The Server Control module includes components and tools that allow you to:

1. Deploy policies to endpoints.
2. Define resources
3. Define accessors
4. Define access levels

VII. Cyberark Pam
CyberArk's Privileged Access Manager (PAM) is a full-lifecycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control, and monitor all activities associated with all types of privileged identities. Looking at different aspects of CyberArk from end user perspective.

1. View and connect with privilege accounts
2. Connect to targets when check-out/check-in exclusive access is enforced
3. Connect to targets when dual control is enforced.
4. Connect to targets using native tools

As an end user one is required to log in and interact with different systems and software. One must provide and remember multiple passwords. In many cases the systems one logs in holds privilege information such as customer information or company information. When one has access to privilege information it makes one privilege user and unfortunately a prime target for attackers. Usually, the attacker goes behind the credential of a privilege user as that is what they need to access the IT infrastructure. Over the years companies have asked their privileged users to come up with strong passwords and to keep those passwords confidential. However, this is insufficient as it is hard for most of us to memorize complex passwords. And attackers these days can crack any password. This is where the PAM solutions can help.

A. Windows administrator (WA)
An extremely qualified windows administrator knows the importance of security because he has access to so many critical systems. To be secure from bad actors one needs to be vigilant. Using complex, unique passwords for all the systems being accessed is important and routinely getting those passwords rotated is part of security policy. Memorizing complex passwords and changing them on a regular basis makes life tough. One may know the threat and take it upon oneself to do all that is needed to make the organization safe.

B. Developer
A developer needs to access explore different systems as part of their learning journey and finding solutions to the programming problems. They don't have access to any production system and may not be victims of a breach. There is a need for the role for accessing multiple online forums to share knowledge and ideas with many fellow developers.

C. Threat
A developer clicks on a link received in an email from an online forum not fully reviewing the message. By doing so, malware was introduced to the system. The malware harvests credentials sitting on the system including those of a desktop administrator who helped the developer to install a new printer driver. Using the stolen desktop administrator credential the malware spreads to many other workstations including a windows administrator (WA). The malware installs a key-logger on WA's system and captures the credential while he is doing his work. Suddenly several critical systems are vandalized using WA's credentials. WA who is ever careful is upset for being the victim of a breach. Because it is WA's credentials that were used management is looking at him for answers. In-spite of doing nothing wrong, the WA managed to become a victim. The developer had no ill intentions either. This can happen to any one of us in our day-to-day activities.

D. Solution
CyberArk Privilege Access Manager can be a solution to prevent such attacks. How will the day-to-day activities of Windows Administrator and the developer be different after the implementation of CyberArk PAM? May be layers of security and slow things down. Here are the benefits:

1. No longer need to remember long and complex passwords
2. Changing passwords is easy and can be done more often
3. Prevents one from being a victim of social engineering,

one cannot reveal the password one does not know.

Conclusion: IAM, IGA and PAM address the risk pertaining to people access, digital identity, privileged accounts in an enterprise. IAM is the discipline that enables the right individuals to access the right resources at the right times for the right reasons. IGA means leveraging the most intelligent and efficient path to mitigating identity risk in the business. IGA is considered to be part of IAM. Omada is one of the many IGA solutions discussed here. PAM is a critical security control that enables organizations to simplify how they define, monitor, and manage privileged access across their IT systems, applications, and infrastructure. CyberArk or Symantec both have great features for an organization's secure usage of privilege accounts based on the enterprise needs.

References

1. FORTRA. What is the difference between IAM, IGA and PAM? [Internet]. Core Security; 2020 Jul [cited 2025 Mar]. Available from: https://www.coresecurity.com/blog/whats-difference-between-iam-iga-and-pam
2. Microsoft. What is Identity Access Management [Internet]. Microsoft Security; [cited 2025 Mar]. Available from: https://www.microsoft.com/en-us/security/business/security-101/what-is-identity-access-management-iam
3. Omada. IGA for Enterprise [Internet]. Omada Identity; [cited 2025 Mar]. Available from: https://omadaidentity.com/products/omada-identity-cloud/
4. Broadcom. Symantec Security Software [Internet]. Broadcom TechDocs; [cited 2024 Nov 21]. Available from: https://techdocs.broadcom.com
5. Broadcom. Modernize the credential vault – Extend privileged access controls to protect secrets, enable DevSecOps, and enforce zero trust architecture [Internet]. Broadcom Identity and Access Management; [cited 2024 Nov 21]. Available from: https://www.broadcom.com/products/identity/pam
6. Broadcom. Symantec Enterprise Blogs/Product Insights [Internet]. Symantec by Broadcom; 2021 Mar [cited 2025 Mar]. Available from: https://www.security.com/product-insights/role-symantec-privileged-access-management
7. Broadcom. Symantec PAM Overview [Internet]. YouTube – Symantec by Broadcom; 2023 Dec [cited 2025 Mar]. Available from: https://www.youtube.com/watch?v=i7l6tqYb0KA
8. Marti R. Beyond the vault – where to take your PAM Implementation next with Symantec [Internet]. Symantec by Broadcom – Product Insights; 2021 Sep [cited 2025 Mar]. Available from: https://www.security.com/product-insights/beyond-vault-where-take-your-pam-implementation-next-symantec
9. CyberArk. Benefits of CyberArk Solution and how to use it [Internet]. CyberArk Training; [cited 2024 Nov 21]. Available from: https://training.cyberark.com/pages/108/privilege-cloud-administrator
10. CyberArk. Breaking down the business benefits and cost savings of CyberArk Privileged Access Management as a service [Internet]. CyberArk Blog; [cited 2024 Nov 21]. Available from: https://www.cyberark.com/resources/blog/breaking-down-the-business-benefits-and-cost-savings-of-cyberark-privileged-access-management-as-a-service

Let me know if you'd like these references alphabetized, numbered differently, or formatted for a reference manager tool.

IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.