Privilege Access Governance

Close the gap between privileged access - and standard-user identities

ONE IDENTITY by Quest

The term **'privileged access management'** – often interchangeable with **'privilege account management'** – is a hot topic lately. It seems that nearly every day there is news of another data breach that eventually is tied to misuse or poorly protected privilege account credentials. Misuse of privilege access makes it is relatively easy for bad actors to gain access or steal sensitive data. Unfortunately, it often takes months, or even years, to detect and then investigate these incidents. By then, the thief and data are long gone.

So, how do you determine which accounts are privileged and how to do you track which individuals in your company have access to those privileges accounts?

One may say that any account that can access personal identifiable information (PI), financial or confidential corporate information should be considered as privilege accounts. However, every organization has to determine what data is privileged to them, which accounts are privileged, where each is located, and who has access to these privilege accounts. Control of these privileged accounts plays a major role in compliance – and governance.

The access control of these privilege accounts, has long been fulfilled by Privilege Account Management (PAM) technologies. However, traditional PAM technologies often are standalone solutions that are not integrated with identity governance and administration (IGA) technologies, which significantly hampers control, visibility and governance of users and access to privileged resources.

PAM systems were designed to offer scalable and secure methods to authorize and monitor privileged accounts across all of your systems. Their main focus has been:

- **Granting privileges** to users
- **Managing one-off privileged access** needed to complete a specific task
- **Controlling access** to privileged passwords
- **Tracking all privileged activity** for reporting and audits of privileged access

Benefits

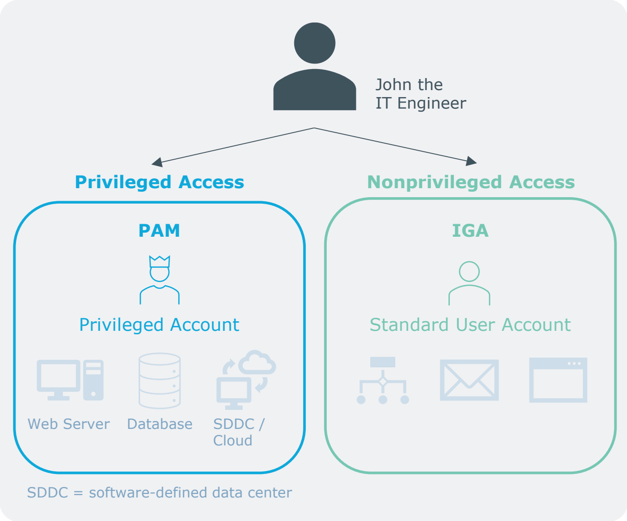
- **Unify identity management** and provisioning processes
- **Eliminate silos** and increases security
- **Simplify compliance**
- **Centralized policy administration** and SoD enforcement
- **Consistent access governance**
- **Eliminate redundant**, improper and excessive access

However, because the non-integration of PAM and IGA systems, line-ofbusiness and privileged accounts are managed separately with separate tools. IAM workloads that must be managed – namely access request, fulfillment/ provisioning, process automation, and attestation/certification – operated independent of each other, which at the very least doubles the management effort.

When these workloads are segregated, true governance cannot take place. Typically, achieving excellence in standard-user governance does not translate to privileged access. However, IGA needs exists across the board. Just because it is harder, or requires separate processes and technologies, doesn't mean governance doesn't apply to privileged accounts and administrative access.

Organizations that operate PAM and IGA technologies in silos (as shown in Figure 1), cannot execute identity provisioning processes with privilege accounts, nor can they enforce cohesive access policies and governance practices. It's impossible to have a single 360-degree view of all identities, entitlements and activity.

There's no reason why you shouldn't get a complete view of all your identities and rights, from standard-user to privileged users. One Identity's Privileged Account Governance (PAG) feature bridges the management gap. It is part of the One Identity Manager offering, which is our full-featured IGA solution.



SDDC = software-defined data center

Figure 1. *PAM and IGA managed separately restricted to the personal use of John the IT Engineer.*

Existing One Identity Manager customers can integrate their PAM technologies into One Identity's IGA platform. This enables them to use account provisioning and access governance capabilities of an IGA system, while continuing to leverage their comprehensive privilege account, access- and session-management capabilities of PAM technologies.

And if your organization uses both Identity Manager and One Identity Safeguard, the PAG feature consolidates management of them to ensure all users of privilege accounts gain and maintain the appropriate level of access to those accounts and credentials.

The benefits of integrating these two solutions include:

- **A central repository** to manage all accounts (privilege, and non-privilege)
- **Unified Identity Lifecycle** management and provisioning processes that eliminate administration silos.
- **Simplify Compliance and Governance** with centralized policy and administration
- **Consistent access-governance processes** that eliminate redundant tasks and enforce separation of duties (SoD) policies
- **A streamlined user experience**

The PAG capabilities bring together the One Identity Manager and One Identity Safeguard solutions.

One Identity Manager simplifies the management of user identities, access permissions and security policies. It mitigates risk, secures data, and helps to meet uptime requirements and satisfy compliance by giving users access to the data and applications that they need to do their work. IGA can be driven by business needs, not IT capabilities. Plus, you can unify security policies.

One Identity Safeguard takes the stress out of protecting your privileged accounts by securely storing, managing, recording, auditing and analyzing privileged access.

Safeguard can detect and halt unknown threats while satisfying your auditors and admin.
It is an integrated solution that combines a secure hardened password safe and a session management and monitoring solution with threat detection and analytics.

Conclusion

You can greatly simplify management of all identities – privileged- and standard-users – with a single tool. One Identity Manager's Privileged Account Governance (PAG) feature brings together your entire environment by closing the gap between how you manage and control access to privileged resources and line-of-business resources.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.