CONNECTING ACCESS GOVERNANCE AND PRIVILEGED ACCESS MANAGEMENT

ABSTRACT

Identity and access governance should be deployed across all types of users associated with an organization -- not just "regular" users but also "privileged" users. Managing regular users separately from privileged users can open your organization up to risk, create security gaps and deprive your organization of a complete view of identity context for access-related decisions.

Managing privileged users and auditing their access is no longer optional, based on regulatory compliance requirements and as evidenced by the spate of recent major data breaches, all of which occurred due to misuse of privileged access.

This white paper will review why connecting a Privileged Access Management (PAM) solution to an access governance solution will enable you to holistically control and audit access to your intellectual property, regulated information and infrastructure systems.

January 2015

RSA WHITE PAPER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Organizations today are struggling with managing and governing access. Increasing regulations, a heightened threat landscape, insider threats and an explosion in the number and type of users have all conspired to cause tremendous pressure on IT and Information Security. At the same time, organizations are expected to grow, generate more revenue and be more productive, which all rely on effective identity and access governance.

Managing and governing identities has become ever more important. Organizations are beginning to understand that all types of users need to be governed in a comprehensive manner; silos of identity management for “regular” users and “privileged” users can cause organizational risk, expose security gaps and deprive the organization of a complete view of identity context. As most highly-publicized data breaches occurred due to misuse of privileged accounts and their credentials, Privileged Access Management (PAM) solutions are increasingly being deployed to help minimize this risk. Automated PAM solutions help organizations meet regulatory compliance requirements, decrease IT risk, increase operational efficiency, and provide advanced privileged audit trails. PAM solutions, via real-time, rapid credential rotation, also help mitigate and contain incidents of hacking and malware attacks.

It is more important than ever to have a unified approach to access governance for controlling access to intellectual property, regulated information and infrastructure systems. As a result, it is advantageous to connect your PAM deployment to an identity and access governance solution. This will provide your organization with a holistic view of identity context, which can then be leveraged to aid in your Security Operations Center (SOC) and Governance, Risk and Compliance (GRC) programs for improved risk remediation and breach investigation.

PRIVILEGED ACCESS MANAGEMENT

Organizations have deployed PAM solutions to protect critical assets and meet compliance requirements by securing, managing and monitoring privileged access, accounts and credentials. Privileged identities typically allow unrestricted access to view, copy and change data, alter configuration files and settings, run programs and access critical infrastructure components. These identities grant “super-user” access to virtually every resource on the network, and are typically associated with hardware or software assets (and not with any one user). Because of this, privileged accounts aren’t only associated with individuals; computer application services and even the business applications themselves also use and store privileged credentials in order to authenticate with middleware, databases and other applications.

Auditing and limiting elevated access can help organizations reduce the risks associated with privileged identities and shared accounts. Specifically, PAM helps organizations:

- Mitigate risks from internal and external threats
- Discover and secure privileged credentials, including rotation periodicity, complexity
- Address and correct negative “Administrative Access” audit findings
- Improve their Governance, Risk and Compliance (GRC) posture
- Provide automated reporting to lower recurring costs and uncertainty related to audit preparations
- Establishing controls around privileged access continues to be a high-priority for both organizations and auditors.

CHALLENGES WITH STANDALONE PAM DEPLOYMENTS

Too often, PAM solutions are deployed separately from an identity and access governance solution, creating silos of identity management with inconsistent identity policies. Privileged identities are not incorporated into governance processes like reviews, are not subject to access policies, and/or are not plugged into business processes such as requests and approvals. Further, PAM tools that are not automated can require manual intervention for activities such as provisioning. If PAM solutions aren’t connected with governance, organizations do not have a full view of entitlements and identities and cannot fully reduce access-related risks. An identity is an identity is an identity, and all identities should be governed consistently.

A glaring issue when it comes to requesting, granting and reviewing privileged access is that the line of business is rarely involved. Moreover, privileged users are not just the “in-house” technology management staff! They may be outsourcers, service providers and supply chain partners. Significant damage can also occur from excessive or inappropriate access to business applications that have sensitive data such as SAP, Oracle and JD Edwards, to name a few. IT does not know who should have access to these business applications and what levels of access and entitlements should be granted.

PAM should be tightly woven into governance processes, so that when access to a privileged account is requested, approved or reviewed, the appropriate business context is in place and the entire ‘access control chain’ becomes part of the permanent audit trail.

CONNECTING ACCESS GOVERNANCE TO PAM

As the above examples make clear, you cannot make accurate or effective decisions about access rights without integrating knowledge of the user identities, application access, business context, and resource classification. Organizations that don't have a solid access governance solution in place will fall short of meeting their PAM goals, and will therefore fall short of meeting their broader security goals. In fact, an ineffective PAM solution can lead to both a false sense of security as well as to material audit findings.

To have a truly strong and defensible security practice around access governance, organizations should deploy an integrated PAM and access governance platform, which supports managing access to both business applications and infrastructure systems, in a unified and automated fashion.

A combined solution will provide privileged access visibility by collecting information about privileged access and resources and will provision/de-provision all privileged access. Further, it will provide governance of the PAM application itself, by collecting entitlements, accounts and access information from the PAM application, and provision the access to the PAM solution based upon business policy, ideally based upon automated approval workflows.

Use Case	Access Governance	PAM
Request and grant long-term privileged access	Yes	No
Review, certify and remediate who has access	Yes	No
Business Context for Request, Approval, Policies	Yes	No

As the above figure demonstrates, organizations need to integrate their access governance and PAM solutions for the above use cases. PAM on its own creates holes for requesting and granting long-term privileged access; reviewing, certifying and remediating who has access; and lacks business context for access request, approval and associated policies.

BENEFITS OF A COMBINED SOLUTION

Combining PAM and identity governance will enable your organization to have a full view of who has access to what, no matter if these resources are business applications or critical infrastructure components. By collecting PAM entitlements into the governance platform, you can control all privileged access based upon business processes and policies (both risk- and governance-driven), such as access reviews. You will be able to provide automated controls over the request, approval and provisioning of privileged entitlements. Having a centralized approach to governing identities can also enable you to leverage identity intelligence in your Governance, Risk and Compliance (GRC) and Security Operations Center (SOC) programs.

You can expect to achieve the following benefits:

- Provide a single control point for provisioning all identity access within the enterprise
- Limit access and gain visibility into all privileged usage, in all silos in the datacenter
- Streamline the on- and off-boarding of internal and external users
- Identify users with excessive access to business applications and infrastructure systems; reduce the risk of insider threats
- Integrate with an automated certification process to allow compliance teams to track admin risk and allow the line of business to make access decisions
- Identify segregation of duties violations and risks
- Integrate with the request, approval and provisioning processes for automation and an improved risk posture

CONCLUSION

When a PAM solution is integrated with an identity and access governance solution, organizations will gain better visibility and control, and can begin to integrate the rules, processes and workflows across all identities, whether privileged or "regular." Organizations can then make informed access decisions within a proper access governance framework, appropriately evaluate and manage risk, and obtain maximum benefit from their chosen PAM solution.

WWW.RSA.COM