Governing Privileged Access

Creating a single access control chain with IGA and PAM

SailPoint Identity+ Alliance

WALLIX TRACE, AUDIT & TRUST

Governing Privileged Access:

Creating a single access control chain with IGA and PAM

ABSTRACT

The steady drumbeat of highly damaging corporate data breaches along with the increasingly stringent compliance demands legislated in their response means organizations need a way for controlling all access, including privileged, to IT resources more so than ever before. Trends like cloud computing, growth in mobile device use, and a general increase in the threat landscape including the failure of perimeter based security solutions has created urgent pressure to make identity-based security controls even more robust. Many organizations employ specialized Identity Governance & Administration (IGA) systems for this purpose, which also include other beneficial base functionality like providing data for audits of system access. What identity governance solutions don't do is monitor privileged access. PAM controls that kind of access by system administrators who have privileges such as modifying configuration, adding and deleting accounts, and so forth. The truth is out of necessity and legislation both arise a need for system access to be monitored and controlled at every level. Joint IGA-PAM solutions can create a single access control chain by combining the range of identity governance with the specificity and power of inspection of PAM solutions. This paper examines how adding PAM "deep controls" like credential vaulting and rotating to the power of identity governance each serves to extend the potential and value of the other and offers insights into how these two technologies can work together to bolster overall security and compliance.

INTRODUCTION

Identity is elemental to information security and compliance. Who is who in the organization? Who is allowed to do what? Security and compliance managers need to define and enforce access policies based on identity. Mr. X can use System A, but not System B. Ms. Y can use Systems A and B, and so forth.

Identity governance grows more challenging as organizations expand into ever more complex digital enterprises. A new generation of sophisticated Identity Governance & Administration (IGA) solutions offer enterprises a method of meeting increasing security and compliance challenges. While managing user identity, however, the organization must also monitor the parallel process of Privileged Access Management (PAM). PAM involves controlling and monitoring access by those who have administrative privileges. Both identity governance and PAM are necessary today, ideally working together. This paper looks at how a joint IGA-PAM solution can work.

SailPoint
Identity+ Alliance

WALLIX
TRACE, AUDIT & TRUST

IGA OVERVIEW

If you've ever been asked for a username and password in order to log into a site, you've used a simple identity management system. Things can get complicated fast, though. Consider how many applications and user types you might have in a large organization. If you're responsible for security or compliance, how can you be sure that only authorized people have access to IT resources?

IGA should ideally govern access to any and every IT resource. These include applications, databases, storage resources and networks, as well as resources belonging to partners. IGA's job is to mitigate the security and compliance risks inherent in unauthorized access, and protect organizations from data theft, disclosure of confidential information and malicious mischief, among other things.

To defend against these risks, IGA systems generally employ certain core functionality:

- Approvals – governance and management of user identity, access and service requests across the entire identity life cycle.

- Auditing – providing auditing and governance data to enable organizations to meet compliance requirements.

- Policy Checking – automatic, policy-based access in accordance with employee events, including joining, moving or leaving the organization.

- Access Reviews – auditing of usage rights for security and compliance.

There are a number of approaches to implementing identity governance. In some cases, access and identity are governed on a system-by-system basis, while in others each type of access is matched to a specific role. For example, an accounting user can access the accounting system, but not the human resources applications. A business might have access and identity governed at the level of the business unit. Employees of division X can access a set of systems. Employees in division Y cannot, and so forth.

PAM OVERVIEW

PAM governs privileged access. A privileged account has administrative access to the "back end" of the IT resources that everyone else uses. While IGA and PAM slightly overlap, they are also markedly different. A privileged user is able to set up, modify, or delete IT resources. This is sometimes called "root access," which can potentially be dangerous. Through error or malfeasance, a privileged user with root access can wreak havoc on an organization's information assets.

A PAM solution seeks to mitigate the risk of unauthorized privileged access or privilege escalation. It accomplishes this goal by establishing a secure, streamlined way to authorize and monitor all privileged users:

- Granting privileges to users only for systems on which they are authorized.

- Granting access only when it's needed and revoking it based on time and other factors. This is important given that privileged access is often granted to external parties such as IT contractors and vendors. There is no reason for any privileged user to have privileged access after the specific purpose of that access has been served.

- Avoiding the need for privileged users to have or need local/direct system passwords. Direct access to systems frequently means that the privileged user can circumvent the PAM solution. In this case, there is no control nor is it likely that the privileged session is being monitored for a change log and audit trail. This is a huge risk.

- Centrally and quickly managing access over a disparate set of heterogeneous systems.

- Creating an unalterable audit trail for any privileged operation.

Privileged Access Management architectures vary, but most have the following components working together:

- An Access Manager, which controls privileged account access. This is a single point of policy definition and policy enforcement for privileged access management. The Access Manager knows which systems the user can access and at what level of privilege.

- A Password Vault, which uses single sign-on (SSO) and comparable techniques which prevent privileged users from knowing the actual passwords to critical systems. Users cannot view or access their passwords to targeted systems. This prevents manual overriding of a system on a physical device.

- A Session Manager, which tracks what a privileged user actually did during an administrative session.

UNDERSTANDING THE MANDATE FOR BETTER IDENTITY GOVERNANCE

Security and compliance drive improvements in the efficacy of identity governance. This affects both IGA and PAM. Security threats have multiplied in recent years. Business impacts from security incidents have grown more serious, as well. Increasingly virulent threats are posed by cyber warfare, hackers representing sovereign states, organized criminal gangs, and more. Internal threats also abound.

In each case, identity governance and access control are essential to defend against attacks. Attackers frequently try to gain root access by posing as someone within the organization. They may start out posing as a standard user and get upgraded to privileged status. They might create a nonexistent user with special access rights. Or, they will attack directly by assuming root access. In any case, once they have root privileges, the attacker can exfiltrate data, bring systems down, cause embarrassment, and so forth. Indeed, some of the worst data breaches in recent history have involved malicious actors assuming privileged yet unauthorized roles in order to breach protected systems.

Compliance involves identity governance and PAM along multiple threads. The Governance, Risk and Compliance (GRC) frameworks used by most organizations invariably cover identity governance. The reason for this has to do with a basic, but sometimes overlooked aspect of compliance: while the organization is bound by regulations, it is the people who actually do the tasks that make the organization compliant. Therefore, people must be subject to controls that ensure compliance. This objective is realized through IGA and PAM. The following examples demonstrate the intersection between IGA, PAM, and compliance:

- **PCI** – Payment card processing requires many information controls, such as data encryption. Encryption, though, is not a technological abstraction. Someone has to set up the encryption functionality. Someone can modify it or override it. A PCI compliant organization must therefore be able to prove that the people responsible for encryption are properly verified and under effective identity governance. The organization has to ensure that no unauthorized person is disrupting the encryption required to stay compliant. More broadly, PCI compliance means implementing identity-based access controls to limit access to card data to only those employees who require it. The organization also needs to be able to control visibility into card transactions and audit identity-based access logs. This takes an integrated IGA and PAM solution.

- **SOX** – Sarbanes-Oxley requires a review and audit of internal controls that affect financial reporting. Many internal controls are specifically directed at individual system users. For instance, “segregation of duties” may be needed to make sure that a control is effective. Segregation of duties is a mode of control that splits up tasks that can affect a company’s finances between multiple users so that no one user can defraud the business. As an example, segregation of duties might state that a single user may not both create a user and pay a user. An IGA solution can define and enforce this kind of segregation of duties. PAM is needed to make sure that an accounting user cannot override the segregation of duties setup. The financial industry has seen just this kind of problem firsthand. At least one massive banking scandal arose when a bank employee was able to override a trading system by impersonating his manager. Separate controls can work together to mitigate fraud risk. PAM vaults passwords and records sessions to make sure each system is hard to abuse. IGA keeps track of who has access to what and prevents toxic combinations of access via segregation of duty policies, while keeping access fresh and fitted to reflect changing roles as people change jobs.

- **HIPAA** – Guaranteeing the privacy of personal health information means controlling the people who use it. Identity governance solution provision and deprovision access to electronic health records (EHRs). PAM is responsible for protecting root access to systems that store EHRs.

DRIVERS OF INCREASINGLY ROBUST IDENTITY MANAGEMENT

New developments in technology and business exert added pressure on organizations to improve identity governance. Cloud computing, for instance, requires that organizations control access in multiple infrastructure environments, some of which they may not manage directly. Other examples include:

- **Mobility** – The growing use of mobile devices for work, including "Bring Your Own Device" (BYOD) policies, opens up a number of issues for IGA and PAM. Authenticating users of devices not controlled by the organization means extending identity governance onto new platforms. New security use cases arise, as well. What happens if an employee loses his or her personal mobile device, which happens to include access to protected systems? IGA policy and technology must address this scenario, among many other security and compliance implications of BYOD policies.

- **Alliances and partnerships between organizations** – Boundaries between users in different organizations have grown blurrier in recent years. Think about how users at a healthcare insurer and a hospital may need access to the same patient information. How can IGA and PAM control who sees what? Who decides that a user needs to be cut off from access?

- **Multiple classes of workers** – IGA and PAM must contend with many different types of users. Today, organizations have contractors, vendor employees, visitors, and temporary staff who need access to IT resources. Each type or user will likely need his or her own class of access with specific time structures. A guest may need a day-long access to a certain network. A contractor may need 90-day access to a single application.

THE RISKS OF IDENTITY GOVERNANCE SILOS

IGA and PAM complement one another, but when they are implemented separately there can be silos of identity governance. This creates problems for security and compliance and threatens both via maintenance of inconsistent access policies. For example, privileged access may not be subject to reviews established by IGA. A system admin may thus be able to inappropriately access confidential data or restricted processes. Segregation of duties mandated by compliance may easily be compromised in this setting.

Sound identity governance calls for line of business (LOB) involvement in managing access rights. LOB involvement is important because it provides the proper business context to determine who should have access to what. When there are seperate identity silos, their contribution becomes harder to implement simply because the LOB may have no awareness of what privileged access rights exist. IGA forces access approvals to become part of the ongoing business process, which is particularly important when governing privileged accounts. Without IGA, it is hard to properly scale administration of these accounts, leaving IT in a challenging position.

Non-employee access presents another risk. Building on the theme mentioned above, the business needs to address the reality that many privileged users work for someone else. Businesses' most confidential IT resources may routinely be accessible to external IT consultants, freelance software developers, outsourced workers in other countries, vendor technical reps, and more. They may be the most ethical people in the world, but the business won't know who they are and what they are doing. That's a big risk exposure.

Consider the following segregation of duties example: imagine that John is a procurement staffer. As a user of the procurement management system, he can approve purchase orders but he does not have the authority to approve new vendors. That duty is segregated based on policies defined and enforced through an identity governance solution. Only John's manager, Julie, can approve new vendors. This segregation enforces an internal control that prevents a single person from setting up a new vendor and approving a purchase order to that vendor. Without this control, the company is exposed to internal fraud risk.

Now, imagine that John requests privileged access through a PAM solution so he can modify the settings on the procurement system. The IT person responsible for the procurement system manually approves the request, figuring that John has a legitimate reason to access the back end. Julie is not aware that John requested back end access. She doesn't know that he's been granted access and she has no idea what modifications he's made to the system.

This is an internal control failure. Even if nothing bad happens, the lack of visibility and traceability represents a control deficiency. It might get picked up on audit, but it could easily get missed. Beyond compliance issues, the lack of LOB visibility and general oversight into privileged access exposes the company to risks of data theft and more.

THE VISION: A SINGLE IDENTITY GOVERNANCE POLICY

The security and compliance environment calls for a single identity governance policy that includes privileged access management. If this vision can be realized, then a request for privileged access can be managed in accordance with established identity governance policies. This way, all access requests and grants are part of a single access control chain. All access becomes more easily auditable.

Creating a single access control chain

Given that IGA and PAM systems are usually separate, with separate ways of modeling identity and controlling access, how can there be a single access control chain? The answer involves leveraging a joint IGA and PAM solution that centralizes identity governance to include privileged access management with a single, authoritative identity store. The IGA system can now be set up with automated workflows that require manager approval of any access requests, including requests for privileged access.

Returning to the example, what if John changes departments? A joint IGA-PAM solution can flag the fact that John should not have his old procurement system access privileges if he is no longer working in procurement. If he is able to retain his admin rights to the procurement system even if he leaves the department, the internal control will be deficient. When John requests privileged access to the procurement system through the PAM solution, his transfer will trigger a review and approval of his access privileges by Julie. She may or may not approve the request, but she will at least be aware of it and can flag any segregation of duty violations. Alternatively, the IGA system could establish access approval rules that deny privileged access requests that violate segregation of duties or other access governance policies. The rules contained in the request approval workflow can be shaped by identity governance policies.

Changes to John's access privileges

John's PAM approval request can tell Julie whether John is a full time employee or a contractor, and so forth. The requests and grants of access are recorded on a central audit log. If Julie approves John's request, the PAM solution will then log any of his privileged account sessions, something that most IGA solutions are not set up to do.

Architecturally, a joint IGA-PAM solution could be integrated in several different ways. Most industry experts favor an approach that bases PAM functions on a central identity store managed by the IGA solution. With this approach, there is just one master set of identities to manage for both general access and privileged access. The IGA solution can also house a comprehensive audit log of all access requests, including privileged access requests.

BENEFITS OF THE JOINT IGA-PAM SOLUTION

Done right, a joint IGA-PAM solution protects a company's most critical data and IT assets better than having separate IGA and PAM identity silos. It improves the overall GRC posture.

Benefits include:

- Having a single point of control and access control chain for provisioning all access in the organization.

- Ensuring that privileged access sessions are performed in accordance with an organization's governance policy.

- Enabling auditors to more easily discover inconsistencies in access authorizations, including segregation of duties violations and other role-based access restrictions.

- Identifying users with excessive access to highlight potential insider risks.

- Streamlining the process of on-boarding and off-boarding of all users, both internal and external.

CONCLUSION

Identity governance is one of the few things that security and compliance managers can count on to both combat the changing and dangerous threat landscape and meet growing compliance demands. The most serious security threats now involve manipulation of identity. IGA solutions offer a way to govern who has access to what, but they generally lack deep the deep controls – such as credential vaulting and session recording – that are needed to increase the security of privileged accounts. A PAM solution offers a secure, streamlined way to authorize and monitor all privileged users for all relevant systems. A joint IGA-PAM solution can mitigate identity governance risks better than either IGA or PAM on its own by extending the reach of traditional identify governance and preventing breaches associated with privileged access. IGA and PAM vendors are now collaborating closely on joint solutions for full identity governance that create a single access control chain capable of monitoring and controlling system access at every level. This not only dramatically improves security, but also means access becomes more easily auditable, enhancing an organization's ability to meet its compliance challenges.

WALLIX
TRACE, AUDIT & TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX ADMINBASTION Suite. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: **@wallixcom**

www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email: deinfo@wallix.com
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré $7^{\text{ème}}$ Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

SailPoint
Identity+ Alliance

WALLIX
TRACE, AUDIT & TRUST