SafePaaS™

Understanding Access Governance: A Complete Guide

Beyond RBAC – How Fine-grained PBAC Controls Drive Business Success in a Digital Platform.

Contents

- Understanding the Difference Between Access Management and Access Governance
- The Shortcomings of First-Generation Identity Governance
- The Future of Identity Governance - Policy-based Access Governance
- Capabilities of a Modern Access Governance Solution
- How SafePaaS Supports Modern Access Governance Requirements

Understanding the Difference Between Access Management and Access Governance

Access Management

Access Management, or Identity and Access Management (IAM), is a critical component of organizational cybersecurity often confused with Access Governance. While related, these concepts serve different purposes within the security framework.

Key Components of Access Management

Authentication

Uses various methods to verify the identity of users, systems, or devices like:

- Usernames, passwords, and biometrics
- Multi-factor authentication (MFA)

Authorization

Determines user permissions after authentication based on:

- Roles and responsibilities
- Specific permissions
- Principle of least privilege

Single Sign-On (SSO)

- Enables access to multiple applications with one set of credentials
- Enhances user experience and security
- Reduces password fatigue and potential vulnerabilities

User Lifecycle Management

- Provisioning: Creating new user accounts and granting initial access
- Modifying: Adjusting permissions as roles change
- Deprovisioning: Revoking access when no longer needed or appropriate

Focus of Access Management

Access Management primarily concentrates on the technical and operational aspects of controlling access to digital resources. Its main objectives include:

- Ensuring the right individuals have appropriate access to specific resources
- Implementing and maintaining robust access control mechanisms
- Streamlining user authentication and authorization processes
- Protecting sensitive data and systems from unauthorized access

SafePaaS™

© SafePaaS 2024

Access Governance

Access Governance is a comprehensive, strategic framework that complements and oversees Access Management processes. While Access Management focuses on the operational aspects of controlling access, Access Governance ensures that these processes align with organizational objectives, policies, and compliance requirements.

Key Components of Access Governance

Policy Development and Management
- Creates and maintains access policies
- Defines rules for granting, reviewing, and auditing access rights
- Ensures alignment with organizational goals and regulatory requirements

Segregation of Duties and Sensitive Access
- Establishes policies to prevent conflicts of interest
- Distributes critical functions among different individuals
- Reduces risk of fraud and errors

Periodic Access Reviews (PAR) and Certification / User Access Reviews
- Conducts regular reviews of user access rights
- Ensures access permissions remain appropriate over time
- Aligns with the principle of least privilege

Compliance and Auditing
- Demonstrates adherence to industry regulations and internal policies
- Provides detailed access records and audit trails
- Enhances accountability and transparency

Risk Management
- Identifies and mitigates risks associated with access management
- Prevents unauthorized access and addresses potential security threats
- Aligns access policies with overall risk management strategies

Data Access Controls and IT General Controls (ITGC) Automation
- Tracks changes to key configurations in applications
- Monitors sensitive data access and key transactions
- Oversees master data changes

Focus of Access Governance

Access Governance takes a holistic view of access control, focusing on:

- Aligning access management processes with organizational objectives
- Ensuring compliance with regulatory requirements and internal policies
- Implementing a risk-based approach to access control
- Providing oversight and accountability for access management processes
- Continuously improving access policies and procedures

Access Governance improves security, mitigates risk, and ensures access management processes align with broader business objectives and compliance requirements.

SafePaaS™

© SafePaaS 2024

The Shortcomings of First-generation IGA

Previous Access Governance efforts have consistently failed to keep up with the pace of digitization, cloud adoption, dynamic work environments, growing compliance mandates, and increased cyber security risks.

While traditional Identity Governance and Administration (IGA) systems offer some capabilities, they must be more comprehensive to govern access across the entire organization effectively.

The Role-Based Access Controls (RBAC) used in ERP applications, Identity Governance (IGA), and IT Service Management systems (ITSM) are no longer sufficient to meet the needs of today's digital environment. This is especially true for managing cross-application access based on policies, including Segregation of Duties, User Access Request Orchestration, Periodic Access Review, Privileged Access Management, and Data Protection.

"IGA systems lack fine-grained risk management for compliance, auditing, and security in fast-paced digital landscapes with on-premise and cloud applications and hybrid work models."

Managing and controlling the identities with elevated privileges that can grant users access to ERP systems, enterprise applications, databases, servers, and cloud infrastructure is challenging without effective policy-based access controls. Complex ERP security design can impede the deployment of a modern digital business platform without specialized solutions and knowledge.

SafePaaS™

© SafePaaS 2024

Due to the rise in compliance requirements and greater cybersecurity threats, the demand for efficient access controls has grown beyond the standard capabilities of Identity Governance and Administration (IGA) systems. Consequently, IGA customers now need specific capabilities designed to meet new control objectives and address the shortcomings of general-purpose IGA systems such as:

- They aren´t policy-based.
- They support role-level controls that are continuously changing.
- Lack the ability to configure access rules in terms of fine-grained privileges in the enterprise application security model.
- The focus is on “birthright” access for all user rights, whereas IT audit requires control evidence for enterprise access users with hundreds of privileges to sensitive data, transactions, and functions.
- Lack of support for short-lived, just-in-time elevated access required for emergency support – privileged access management (PAM).
- Single Sign-on to business applications for “birthright” users does not control provisioning fine-grained privileges that v iolate company policies such as Segregation of Duties or Data Privacy.
- The inability to monitor or manage user activity in enterprise applications is required for “lookback” analysis when a risk materializes.
- Unable to support business process owners and control owners need to certify user access or activity log to support periodic access certification.
- There is a lack of functionality to support complete security, and application administrators need to maintain role design and update entitlements to remediate inherent risks in thousands of privileges available in enterprise applications.

SafePaaS™

© SafePaaS 2024

The Future of IGA: Policy-based Access Governance

Policy-based Access Governance (PBAC) is an adaptable and efficient way for organizations to address the challenge of access more efficiently.

Policy-based Access Governance defines access controls through policies based on contextual information. This means access decisions are made by considering factors like user attributes, device information, location, and time of access. Here's why policy-based access governance is better suited for modern, digital organizations:

- **Fine-Grained Control:** Policies allow organizations to set precise, conditional access rules. For example, access can only be granted to a specific application if the user is within the corporate network and using a company-managed device.
- **Adaptive Security:** Policy-based access can adapt to changes in user roles, responsibilities, and the security landscape. It allows for immediate adjustment of access based on evolving needs.
- **Risk Mitigation:** By continuously evaluating risk factors, policy-based access governance helps proactively identify and respond to security threats, reducing the potential for data breaches.
- **Compliance:** Policies can be designed to meet the strictest regulatory requirements, giving organizations greater confidence in their compliance efforts.
- **User Experience:** With policy-based access, legitimate users are less likely to encounter roadblocks, as the system can make more informed, real-time access decisions.

Policy-based access governance offers the agility and precision needed to secure today's complex business environments. Making access decisions based on real-time context and risk factors helps organizations stay ahead of security challenges, adapt to evolving requirements, and ensure compliance.

This forward-thinking approach enhances security, minimizes risks, and simplifies access management in the digital age.

SafePaaS™

© SafePaaS 2024

Key Features of an Advanced Access Governance Solution

With guidance from External Audit firms and Leading Analysts, forward-thinking organizations are turning to policy-based access governance solutions to address complex access challenges.

Access Governance must-have capabilities:

- Segregation of Duties and Sensitive Access Policies
- Policy-based Identity Access Life Cycle Management
- Roles Management - Simulation and Entitlement Management
- Integrated Fulfilment - Support for Access Requests
- Workflow Orchestration
- Access Certification / Periodic Access Review / User Access Review
- Advanced Analytics and Reporting
- Data Access Controls (ITGC Automation)

SafePaaS™

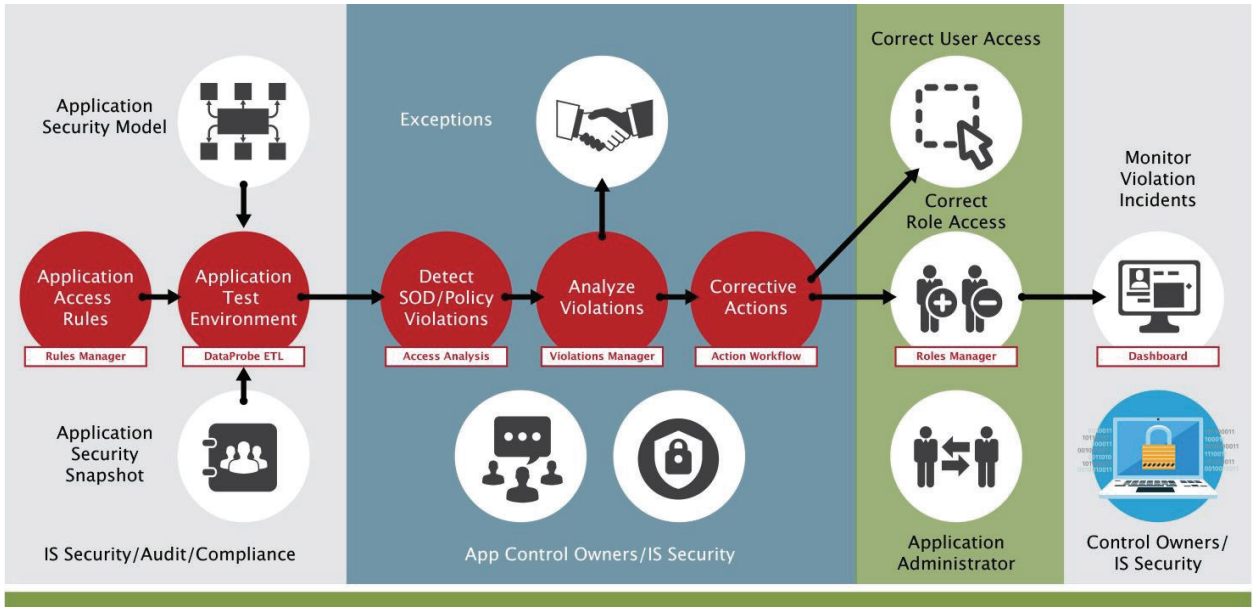
© SafePaaS 2024

Segregation of Duties and Privileged Access Policies – Policy Management

Policy Management is key in detecting access policy violations that could lead to financial, operational, fraud, and cyber risks. An effective solution should allow you to define policies based on risk descriptions, impact, likelihood, and fine-grained rules, utilizing both discrete and fuzzy logic to manage IT system security entitlements and privileges for governance models including Segregation of Duties, Sensitive Access, Data Protection, and Trade Secrets.

To improve risk analysis and response, the solution must eliminate false positives and feature a high-performance policy engine capable of rapidly analyzing millions of security attribute combinations across all enterprise IT systems, ERPs, and business application security snapshots. This ensures accurate and timely reporting of violations.

Violation Management is essential within an SoD solution, enabling the elimination of exceptions where risk is mitigated through compensating controls using advanced filters. Furthermore, Remediation Management issues corrective actions via closed-loop workflows, which expedite risk response, reduce risk exposure, and automatically update violation reports, ensuring accurate and timely audit evidence.

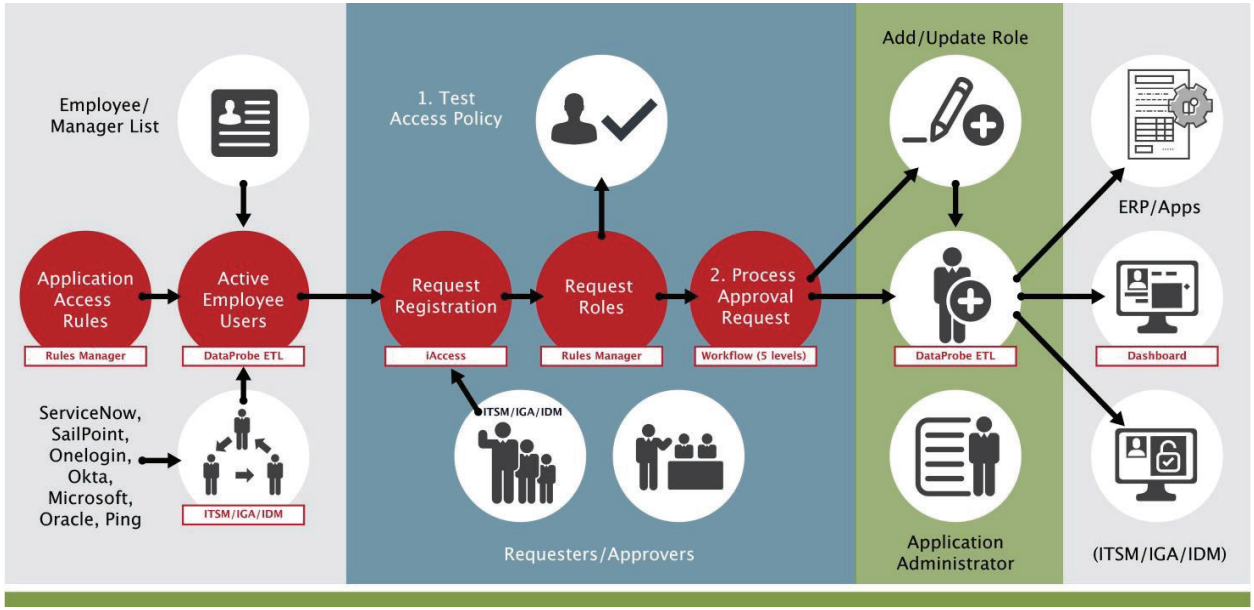


SafePaaS™

© SafePaaS 2024

Policy-based Identity Access Life Cycle Management

Rapid digital transformation, evolving IT environments, and the rise of hybrid work models have significantly increased the risks of managing identity access requests. Organizations with complex enterprise systems, such as an ERP, require Identity Access Life Cycle Management solutions to control access for onboarding and offboarding employees, contractors, and third parties. Any change to work assignments or departures from the organization requires immediate updates to security privileges in compliance with access governance policies to ensure users only have access to what they need while removing access they don't need.



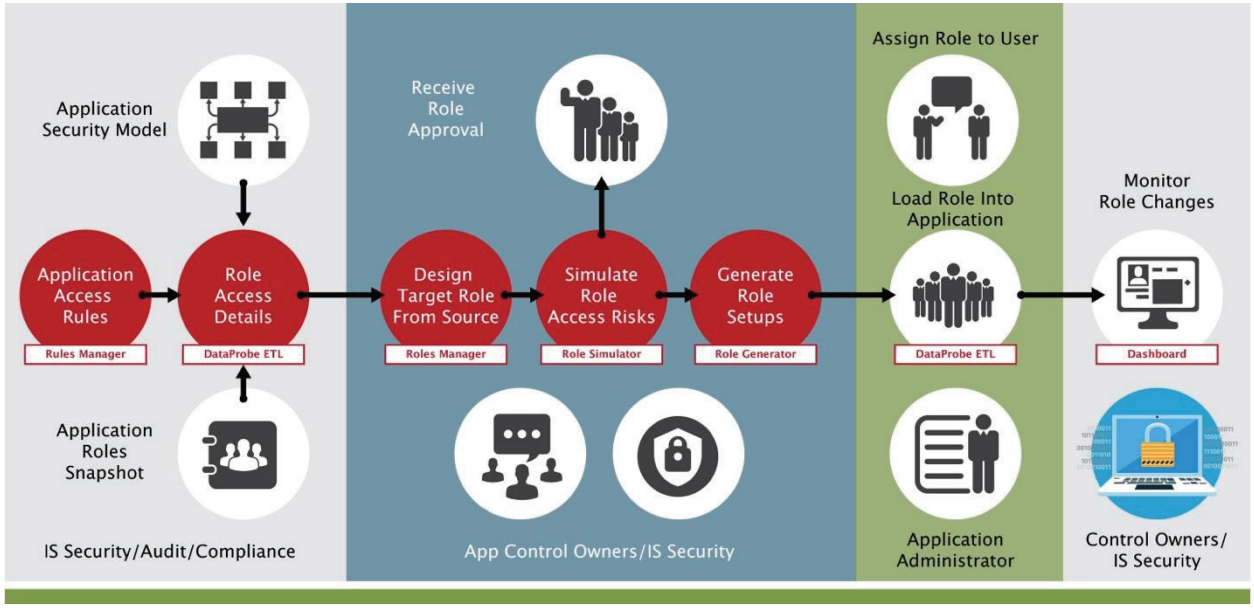
SafePaaS™

© SafePaaS 2024

Roles Management - Simulation and Entitlement Management

Many organizations face challenges in granting business application roles that fit the user access responsibilities and rights to comply with enterprise information policies.

Roles management solutions enable you to automate the design of roles and simulate security scenarios to prevent violations from entering the system. The solution should allow for the identification of role entitlements by analyzing access to application privileges and data within a business application's security structure. Control workflows should ensure that any changes to role designs are reviewed and approved before they are assigned.



© SafePaaS 2024

Integrated Fulfilment – Prevent Risks in ITSM User Request Management

Many businesses use ITSM tools such as ServiceNow to fulfill access requests using roles that are manually configured as catalogs. The downside: **the manual management of roles at a high level create audit findings where the attribute level details in the business application do not accurately reflect in the catalog role.** For example, the Payables Inquiry role available in ServiceNow does not prevent the risk of fulfillment, where the user may also be granted access to the role in Oracle ERP Cloud, which enables supplier creation. This causes a significant risk to financial statements, enabling users to create and pay suppliers.

Streamlined Access Management

When employees join or change roles, an automated system manages their access rights across business applications, integrating with IT Service Management (ITSM) tools. This ensures timely updates, correct privilege assignments, and proper security attributes for each user.

This approach enhances security by limiting access to what users need for their roles and improves productivity through quick access provisioning. The system should automatically add users to ERP systems, assign appropriate rights, and set access start and end dates. Organizations can better control user access by automating these processes while minimizing manual effort.

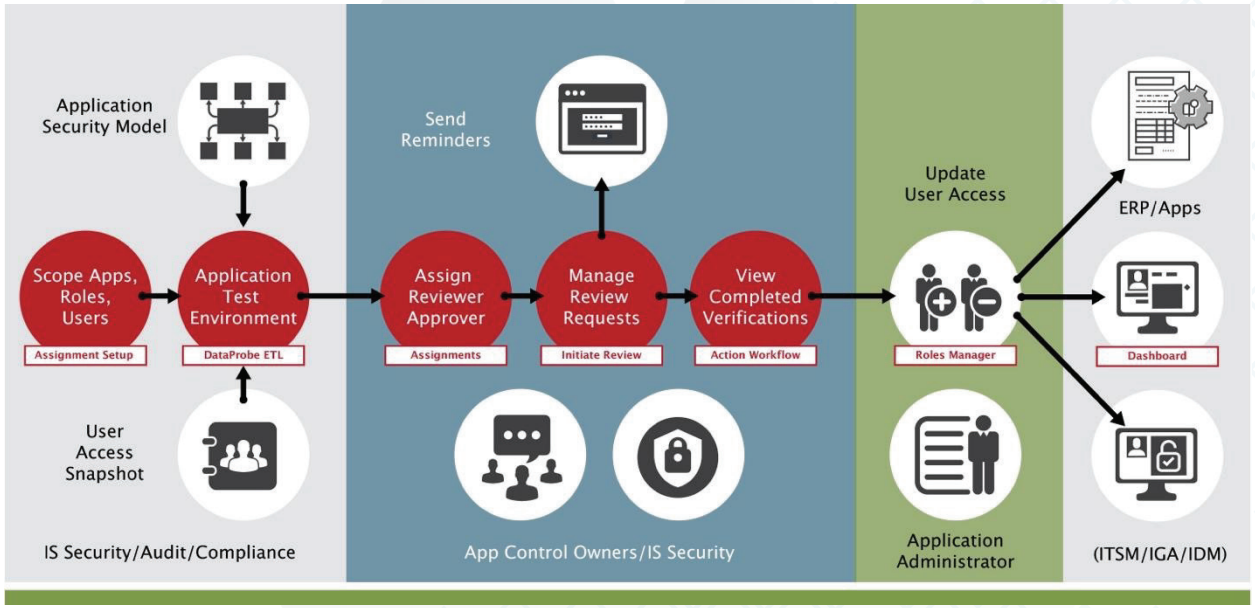
SafePaaS™

© SafePaaS 2024

Periodic Access Review / Certification

Periodic Access Reviews are a necessary safeguard that help protect sensitive data, minimize risk, and ensure compliance. The review process often creates a tremendous burden to collect user access data and send out error-prone spreadsheets, waiting for replies from control managers and process owners.

A periodic access review solution streamlines the access review process with automated workflows to reduce the cost of compliance and mitigate cybersecurity risks.



SafePaaS™

© SafePaaS 2024

Identity Orchestration – Identity Lifecycle Management

Organizations require advanced Identity lifecycle management and analytics integrated into their identity and access management (IAM) platforms to identify and prevent malicious bot activities, cybersecurity threats, and fraudulent risks. This needs to be done without hindering user productivity, especially as organizations move towards a more hybrid digital infrastructure based on the zero-trust model for the digital enterprise.

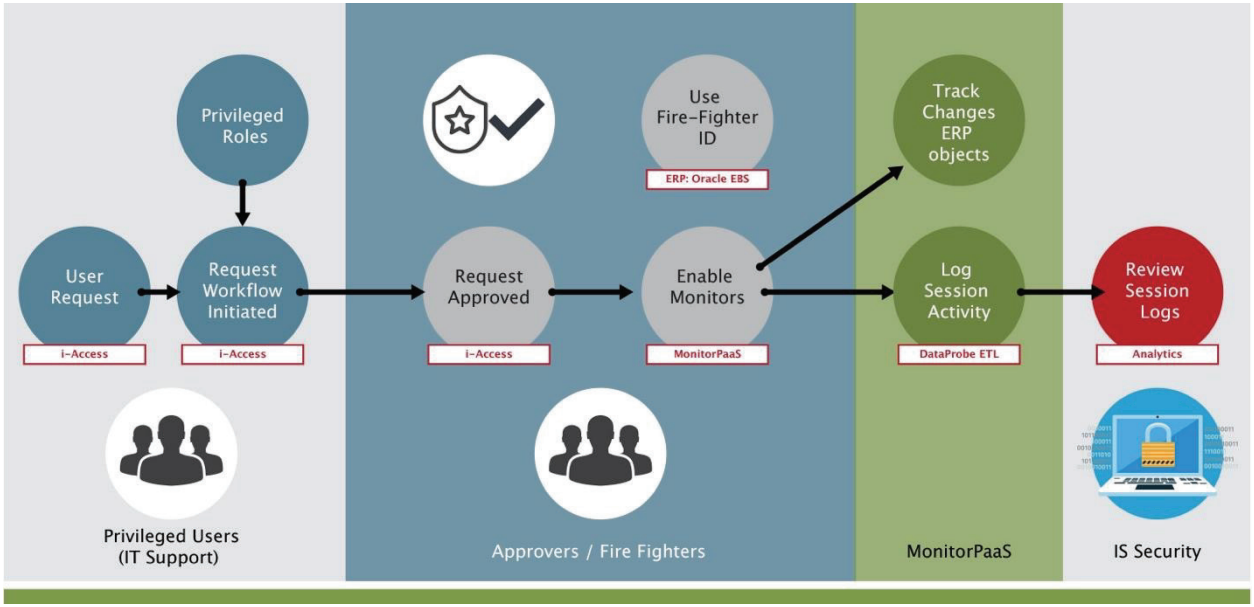
Identity Orchestration enables consistent, policy-based identity and access to all your applications and infrastructure by leveraging current investment in IAM tools like Microsoft Azure/ AD, Okta, OneLogin, Ping Identity, IBM, Oracle, etc. A solution should analyze and control all identities in a distributed model across multi-cloud and hybrid-cloud enterprise platforms. Policy-based Identity lifecycle management ensures that users have authorized access to apps running on-premises or on multiple cloud platforms - whether from the cloud or within the enterprise network - modernizing the identity management process by serving as the orchestration hub allowing siloed identities and distributed policies across fragmented systems to come together for complete visibility.

SafePaaS™

© SafePaaS 2024

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. As organizations rely more on technology and data, the potential for security breaches and data theft increases. It´s key to continuously monitor privileged user and identity activity to ensure the safety and security of data and resources. Privileged users, such as system administrators, have access to sensitive data and can potentially misuse their access to steal data or cause harm to the organization. Monitoring their activities can help you detect any suspicious behavior and prevent security breaches before they occur.



SafePaaS™

© SafePaaS 2024

Advanced Access Analytics - Security Risks and Policy Violations Analysis

Access Analytics is a key component of an enterprise access governance solution. It can improve the effectiveness of controls and provide insight into emerging threats. By monitoring access policy violations, access analytics safeguards against cyber security risks and insider threats.

Analytics is a catalyst for digital strategy and transformation, enabling timely and precise design of business roles and application entitlements in complex, fast-changing business contexts to optimize productivity.

Data-driven organizations can use the Identity data stored in the information system using analytics to ensure successful digital transformation, including policy-based access governance for sustainable value creation.

Organizations need to regularly analyze emerging threats to their business applications and IT systems to support their evolving business requirements, such as hybrid, agile, and hyper-automation. Traditional business intelligence and reporting tools are unable to effectively connect security meta-data changes with the decentralized provisioning process. Effective analysis requires consideration of the privileges assigned to employees, third parties, service accounts, and BOTS to ensure compliance with access governance policies.

SafePaaS™

© SafePaaS 2024

Enterprise Security Data Lake

Exponential growth in data volumes and rapidly increasing attack surfaces are challenging security teams to control cyber threats and data leaks. Security data lakes can help address the key security challenges facing organizations.

The massive data generated from Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions can take days to analyze, and it's cost-prohibitive to store all the collected data, which can cause key signals to be missed during an investigation or breaches to go unnoticed.

Data Access Controls (ITGC automation)

These controls involve tracking changes to key configurations in the applications that support sensitive data, key transactions that create risk in the business, and master data changes.

SafePaaS™

© SafePaaS 2024

How SafePaaS Elevates Modern Access Governance Requirements

The SafePaaS platform offers comprehensive access governance capabilities, including:

Fine-Grained Segregation of Duties (SoD) and Privileged Access Policies: Apply detailed policies across any application, with support for cross-application SoD controls.

Roles and Entitlement Management: Manage access rights for both human and non-human identities, ensuring compliance with enterprise policies.

Access Request Management with Preventive Controls: Streamline access provisioning while preventing unauthorized access through policy-based controls.

Periodic Access Review: Conduct fine-grained reviews across all data sources, including databases and servers, to satisfy auditor requirements and deliver strong security measures.

Privileged Access Management: Implement just-in-time and unified PAM capabilities to secure elevated access privileges.

Data Access Controls: Enable Continuous Controls Monitoring (CCM) for transactions, configurations, and master data.

Segregation of Duties and Privileged Access Management

SafePaaS provides a powerful policy management framework that underpins its Segregation of Duties (SoD) solution. This feature allows organizations to define and manage precise policies and rules governing user access within ERP systems, preventing conflicts before they occur.

The platform supports a comprehensive library of ready-to-use SoD rulesets tailored for major applications like Oracle, SAP, Workday, and Microsoft Dynamics, tested and validated by leading audit firms. These rulesets help organizations comply with key regulations, including SOX, GDPR, and HIPAA.

SafePaaS™

© SafePaaS 2024

Identity Access Lifecycle Management

SafePaaS automates Identity Access Lifecycle Management, enhancing productivity and security by streamlining access request processes. The solution integrates with IT Service Management (ITSM) tools like ServiceNow and Identity Management (IDM) systems like SailPoint and Okta, reducing help desk costs and minimizing errors in access provisioning.

By leveraging advanced workflows, SafePaaS provides real-time visibility into user and identity behavior, ensuring access rights are continuously aligned with organizational policies.

Integrated Fulfillment for ITSM User Request Management

SafePaaS integrates with ITSM systems to manage user access requests comprehensively. All access requests are analyzed against governance policies before fulfillment, with automatic ticket creation and continuous syncing between SafePaaS and the ITSM system. This integration ensures that access requests align with established policies, mitigating risks such as SoD violations and enhancing overall security.

Fine-grained Periodic Access Reviews

SafePaaS simplifies the Periodic Access Review process by fully automating access reviews across applications and data sources for all identities. The platform enhances existing IAM and IGA systems by providing a comprehensive layer of access management controls.

By integrating with tools like Azure, Okta, and SailPoint, SafePaaS ensures the accuracy and completeness of access reviews, reducing the risk of control failures and ensuring continuous compliance.

Roles Management and Entitlement Simulation

SafePaaS offers an advanced roles management tool that includes a catalog of pre-configured roles designed to comply with SoD and data access policies.

Users can simulate and design roles, review potential risks, and finalize roles through automated workflows. This capability ensures that roles are aligned with job responsibilities and compliant with segregation of duty requirements before they are assigned to users.

© SafePaaS 2024

Privileged Access Management (PAM)

SafePaaS provides a robust PAM solution that securely manages privileged access across multiple systems. The platform allows for just-in-time access requests, ensuring that elevated privileges are granted only when necessary and logged for audit purposes.

Integrated with SafePaaS' Identity Access Request Management, PAM helps organizations reduce access risks while maintaining comprehensive control over privileged activities.

Advanced Access Analytics and Security Monitoring

SafePaaS equips audit and compliance teams with advanced analytics tools to monitor and assess security risks, policy violations, and the effectiveness of access controls.

The platform enables auditors to identify discrepancies between approved access requests and actual granted access, providing actionable insights to mitigate risks such as financial misstatements and cyber-attacks.

Continuous ITGC Automation with Data Access Controls

SafePaaS embeds continuous monitoring within its governance framework to track key configuration, transaction, and master data changes. This feature automatically captures detailed audit trails, including who made changes, what changes were made, and when they occurred, ensuring that organizations maintain control over their critical data and comply with regulatory requirements.

SafePaaS is uniquely positioned to meet the modern access governance needs of organizations with complex IT and ERP environments. Its comprehensive platform of solutions enables organizations to embrace access governance, ensure control effectiveness, and mitigate risks effectively.

To learn more about how SafePaaS can help you with Access Governance please contact:

Emma Kelly
Senior Marketing Manager
emma.kelly@safepaas.com

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

SafePaaS™

© SafePaaS 2024