OBSERVEID

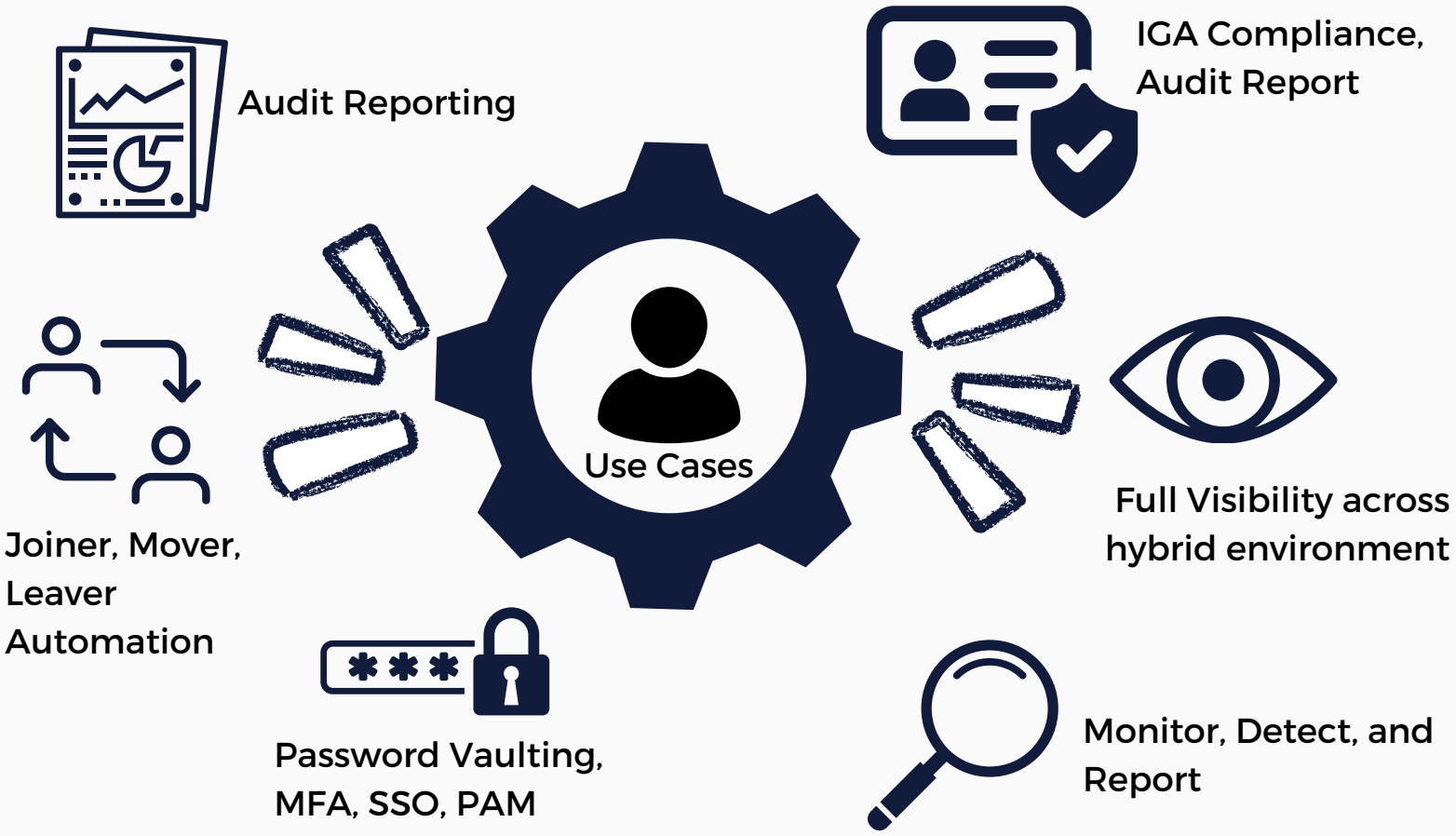
Key Use Cases in IAM, PAM, IGA, and Converged Identity

WHITEPAPER PREPARED BY:

Sperry Bilyea

Table of Contents

Key Use Cases in IAM, PAM, IGA, and Converged Identity



Introduction

As digital transformation accelerates, organizations face increasing complexity in managing identities, access, and governance across hybrid IT infrastructures. Traditional approaches to identity and access management (IAM), privileged access management (PAM), and identity governance and administration (IGA) have become fragmented, leaving organizations vulnerable to security risks and inefficiencies. This whitepaper explores the key use cases across IAM, PAM, and IGA, and highlights the growing need for a Converged Identity Security Platform that integrates these functionalities into a cohesive framework to enhance security, streamline processes, and ensure compliance in modern IT environments.

1 Identity Access Management IAM Main Use Cases

IAM is the foundation of modern identity security, providing the tools and processes required to manage digital identities and control access to applications, systems, and data. Key use cases include:

1.1 User Lifecycle Management

- **Challenge**: Managing the full lifecycle of users—onboarding, role assignment, access modification, and offboarding—across on-premise and cloud environments is complex and often manual.
- **Solution**: IAM automates user lifecycle processes, ensuring users are provisioned and de-provisioned promptly based on role changes or exit, reducing the risk of unauthorized access and improving operational efficiency.

1.2 Single Sign-On (SSO)

- **Challenge**: Users are required to manage multiple credentials for different applications, leading to password fatigue and security risks.
- **Solution**: IAM provides SSO capabilities, enabling users to access multiple applications with a single set of credentials. This simplifies the login process and reduces the risk of weak or reused passwords.

1.3 Multi-Factor Authentication (MFA)

- **Challenge**: Passwords alone are not sufficient to protect against credential theft and breaches.
- **Solution**: MFA enforces additional authentication steps, such as biometrics, tokens, or SMS codes, ensuring that users are authenticated securely before gaining access to critical applications or data.

1.4 Adaptive and Risk-Based Authentication

- **Challenge**: Organizations need to balance security with user experience by adjusting authentication requirements based on user behavior and risk levels.
- **Solution:** IAM provides adaptive authentication, which adjusts authentication requirements based on factors like location, device, and user behavior. For example, users logging in from unfamiliar locations may be prompted for additional authentication.

2 Privileged Access Management PAM Main Use Cases

PAM focuses on controlling and monitoring access to critical systems by privileged users, such as administrators, developers, or service accounts. Effective PAM solutions prevent misuse of privileged accounts and reduce the attack surface for cybercriminals.

2.1 Privileged Session Management

- **Challenge**: Privileged users often access sensitive systems without sufficient monitoring, leading to potential insider threats or unauthorized access.
- **Solution**: PAM enables privileged session management, which records, monitors, and logs privileged user activity in real-time. Organizations can terminate sessions if suspicious behavior is detected, ensuring accountability for privileged actions.

2.2 Just-in-Time (JIT) Privilege Elevation

- **Challenge:** Privileged accounts often have persistent access, increasing the risk of misuse or exploitation by attackers.
- **Solution**: JIT privilege elevation ensures that users are granted elevated access only when needed, and that this access is automatically revoked after the task is completed. This reduces the attack surface by limiting access to critical systems.

2.3 Secrets Management and Credential Vaulting

- **Challenge**: Privileged account credentials are often stored insecurely, leading to increased risk of theft and misuse.
- **Solution:** PAM solutions provide credential vaulting and secrets management, securing credentials like passwords, SSH keys, and API tokens in a centralized vault. These credentials can be accessed securely and rotated periodically to mitigate risks.

2.4 Privileged Account Discovery

- **Challenge**: Many organizations struggle to maintain visibility over privileged accounts, especially in complex environments with legacy systems.
- **Solution:** PAM can automatically discover and categorize privileged accounts across the entire IT infrastructure, ensuring that all accounts are managed securely and reducing the risk of shadow accounts.

3 Identity Governance and Admin IGA Main Use Cases

IGA ensures that the right users have the right access to the right resources at the right time. It focuses on governance, risk, and compliance (GRC), ensuring that access policies are consistently enforced and that organizations meet regulatory requirements.

3.1 Access Certification

- **Challenge:** Regulatory requirements demand that organizations periodically review user access rights, but manual review processes are time-consuming and prone to error.
- **Solution:** IGA automates access certification, enabling managers and auditors to review and certify user access based on business needs and compliance requirements. This ensures that inappropriate access is revoked in a timely manner.

3.2 Role-Based Access Control (RBAC)

- **Challenge:** Managing access at an individual level is inefficient and can lead to over-privileged accounts.
- **Solution:** IGA enables RBAC, which assigns access based on predefined roles that align with users' job functions. This simplifies access management and ensures that users have only the permissions they need to perform their roles.

3.3 Segregation of Duties (SoD)

- **Challenge**: Organizations must ensure that critical tasks are performed by separate individuals to prevent fraud and errors, but manual enforcement of SoD can be difficult.
- **Solution**: IGA enforces SoD policies, automatically detecting and preventing conflicts of interest by ensuring that users do not have conflicting roles or permissions.

3.4 Audit and Compliance Reporting

- **Challenge**: Demonstrating compliance with regulations such as GDPR, HIPAA, and SOX requires extensive audit trails and reports.
- **Solution:** IGA automates the generation of compliance reports, providing detailed records of access rights, user activities, and policy enforcement. This simplifies audits and ensures that organizations can demonstrate compliance with industry regulations.

4 Convergence of IAM, PAM and IGA

While IAM, PAM, and IGA each address different aspects of identity security, a Converged Identity Security Platform that integrates these functionalities provides significant advantages:

4.1 Holistic Security

- **Problem**: Siloed identity solutions can lead to security gaps, as they often fail to provide full visibility into user activities, access rights, and privileged account usage.
- **Solution**: A converged platform provides a unified view of identity and access, enabling organizations to manage and secure all identities—whether privileged or non-privileged—under a single framework. This holistic approach reduces security risks and ensures consistent enforcement of access policies.

4.2 Streamlined Operations

- **Problem**: Separate IAM, PAM, and IGA solutions increase operational complexity, leading to inefficient processes and duplication of effort.
- **Solution**: A converged platform streamlines identity-related tasks, such as onboarding, access requests, privileged session monitoring, and access certification, into a unified workflow. This reduces the burden on IT and security teams while improving efficiency.

4.3 Improved Compliance and Audit Readiness

- **Problem**: Disconnected identity systems make it difficult to track and report on user access, privileged account activities, and policy enforcement.
- **Solution:** A converged platform provides centralized auditing and reporting capabilities, simplifying compliance with regulatory requirements. Automated reporting tools help organizations maintain continuous audit readiness and respond to audit requests quickly.

4.4 Enhanced User Experience

- **Problem:** Users are often required to navigate multiple systems to request access, authenticate, and manage credentials, leading to frustration and inefficiency.
- **Solution:** A converged platform enhances the user experience by providing a seamless interface for all identity-related tasks, from SSO and MFA to privileged access requests and self-service password resets.

Why You Need to Ensure Converged Identity Use Cases are in Your Research

As organizations navigate increasingly complex IT environments, the need for a unified and converged approach to identity security has never been more important. Traditional siloed solutions for Identity and Access Management (IAM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA) create operational inefficiencies, security gaps, and challenges in compliance. When searching for identity security solutions, it's crucial to prioritize converged identity use cases to ensure your organization can meet both current and future identity security challenges.

Here are the key reasons why converged identity use cases should be a priority in your search for functionality:

6.1 Eliminate Fragmentation and Improve Operational Efficiency

- **Problem:** Siloed identity solutions lead to fragmented operations, where different teams manage separate IAM, PAM, and IGA tools. This creates a lack of communication, redundant processes, and delays in managing identities across the enterprise.
- **Solution:** Converging IAM, PAM, and IGA into a single platform enables streamlined workflows and end-to-end automation. User onboarding, access certification, privileged session management, and audit reporting can be managed from a single interface, reducing the need for manual intervention and improving operational efficiency.

6.2 Enhance Security and Reduce Risk

- **Problem**: Siloed IAM, PAM, and IGA systems often operate independently, creating security blind spots. Without a unified approach, it's difficult to track user access across privileged and non-privileged accounts, increasing the risk of unauthorized access, insider threats, and security breaches.
- **Solution**: A converged identity platform provides holistic visibility into all user activities, whether standard or privileged. This unified approach enhances security by enabling real-time monitoring, automated session recording, and advanced threat detection across all systems. Converged use cases ensure that your security policies are enforced consistently across the entire IT environment, significantly reducing the risk of exploitation.

Why You Need to Ensure Converged Identity Use Cases are in Your Research

6.3 Simplify Compliance and Audit Preparation

- **Problem:** Organizations face stringent regulatory requirements such as GDPR, HIPAA, and SOX, which mandate detailed reporting on user access and activity. When identity solutions are fragmented, gathering audit data across different systems can be time-consuming and error-prone, leaving the organization vulnerable to compliance failures.
- **Solution**: Converged identity use cases include centralized audit trails and automated compliance reporting, ensuring that all user activities—both privileged and non-privileged—are captured and accessible in a single platform. This simplifies compliance processes, reduces the time required to prepare for audits, and ensures that the organization remains audit-ready at all times.

6.4 Support for Modern and Future-Ready IT Infrastructures

- **Problem**: With the rapid shift to cloud services, SaaS applications, and hybrid IT environments, traditional identity solutions may struggle to keep up with the pace of change. Siloed solutions are often not equipped to handle the complexities of modern IT infrastructure, where users require seamless access to both on-premise and cloud resources.
- **Solution:** Converged identity use cases are designed with modern IT architectures in mind. A unified platform that integrates IAM, PAM, and IGA ensures that identities are managed consistently across cloud, on-premise, legacy, and hybrid environments. This future-proofs your identity security strategy by providing the flexibility to scale and adapt as your organization's infrastructure evolves.

Why You Need to Ensure Converged Identity Use Cases are in Your Research

6.5 Simplify User Experience and Reduce Complexity

- **Problem**: When identity management tools are fragmented, users often face cumbersome processes to request access, manage credentials, and authenticate across different systems. This creates friction, increases the likelihood of user errors, and can lead to resistance in adopting security protocols.
- **Solution**: A converged identity platform unifies user-facing processes, such as Single Sign-On (SSO), Multi-Factor Authentication (MFA), and privileged access requests, into a seamless experience. Users can request access, authenticate, and manage their accounts from a single interface, improving adoption and reducing the cognitive load on users.

6.6 Maximize ROI on Security Investments

- **Problem**: Investing in multiple, disconnected identity tools can lead to inefficient spending, as these tools often overlap in functionality but require separate management and support.
- **Solution:** By converging IAM, PAM, and IGA into a single platform, organizations can consolidate their security investments, eliminating redundancies and reducing the overall cost of managing identities. A converged platform also reduces the need for additional integration, support, and training, ultimately delivering a higher return on investment (ROI).

Conclusion: Converged Identity Use Cases are Essential for Comprehensive Identity Security

As organizations continue to adopt cloud services, expand remote workforces, and manage increasingly complex IT infrastructures, the need for a converged identity security platform becomes clear. Prioritizing converged identity use cases ensures that your organization is prepared to address the full spectrum of identity security challenges, from managing user access and securing privileged accounts to enforcing governance and meeting compliance requirements.

When searching for an identity solution, ensure that the platform can address key converged use cases across IAM, PAM, and IGA. This unified approach will not only enhance your security posture but also streamline operations, simplify compliance, and deliver significant cost savings over time.

For more Info:

For more information on how ObserveID can help your organization implement UBA and automation, please contact us at **confidence@observeid.com**

References:

1. Forrester Research: "The Future of Identity Security: Why Convergence is Critical" Forrester Identity Security
2. Gartner: "Top Trends in Identity and Access Management" Gartner IAM Trends
3. Identity Management Institute: "The Role of PAM in Modern Identity Security" Identity Management Institute PAM
4. CSO Online: "Why Identity Governance is Key to Cybersecurity and Compliance" CSO Online Identity Governance

Why we launched ObserveID

It boils down to one key word: confidence.

With over 100+ years between us in cybersecurity and identity access management, we've seen it all—from working with legacy software to tackling all sorts of behind-the-scenes implementations and projects.

But here's the thing—we saw a gap. The way multicloud and on-prem legacy IT infrastructures were being managed was anything but nimble. Companies were not keeping pace with the fast-moving needs of today's hybrid working organizations.

So, we had a lightbulb moment: what if we could bring everything together, linking the IT infrastructure efficiently unifying all the identities, entitlements and resources into one single plane?

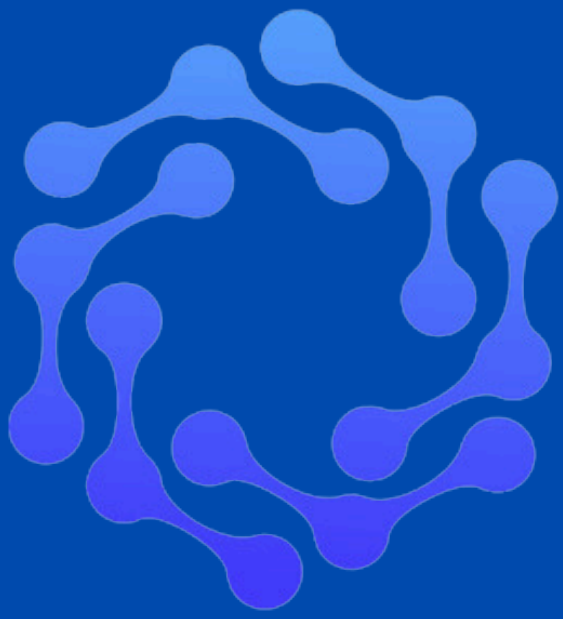
Imagine the boost in confidence for an organization when they know their data is solid, their security risk is under control, and they've got a cost-effective, agile IT infrastructure.

And the real kicker? Ensuring that the right people have the right access to the right information at just the right time.

That's the heart of ObserveID. It's all about giving you that rock-solid confidence in every aspect of your IT environment.

CONFIDENCE

Contact Us



ObserveID

(949) 534-4854
Phone

confidence@observeid.com
Email

www.observeid.com
Website

120 Vantis Drive
Suite 300
Aliso Viejo, CA, US 92656
Address