



OBSERVEID

Building a Secure Future: The Role of Converged Identity in Modern Enterprises

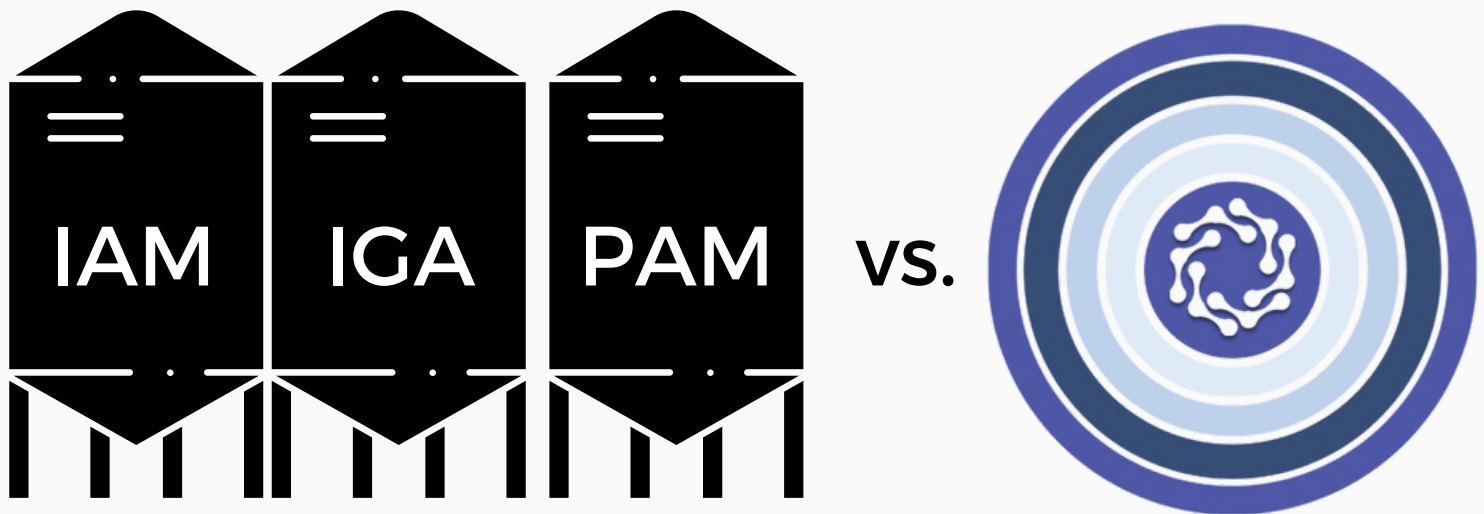
WHITEPAPER PREPARED BY:

Sperry Bilyea

Table of Contents

- 
- 01** Introduction
 - 02** The Benefits of a Converged Identity Security Platform
 - 05** Use Case: Reducing the Surface Attack Area of Hybrid Environment
 - 06** Conclusion: The Future of Identity is Converged
 - 07** References
 - 08** Why we launched ObserveID?
 - 09** Contact Us

Building a Secure Future: The Role of Converged Identity in Modern Enterprises



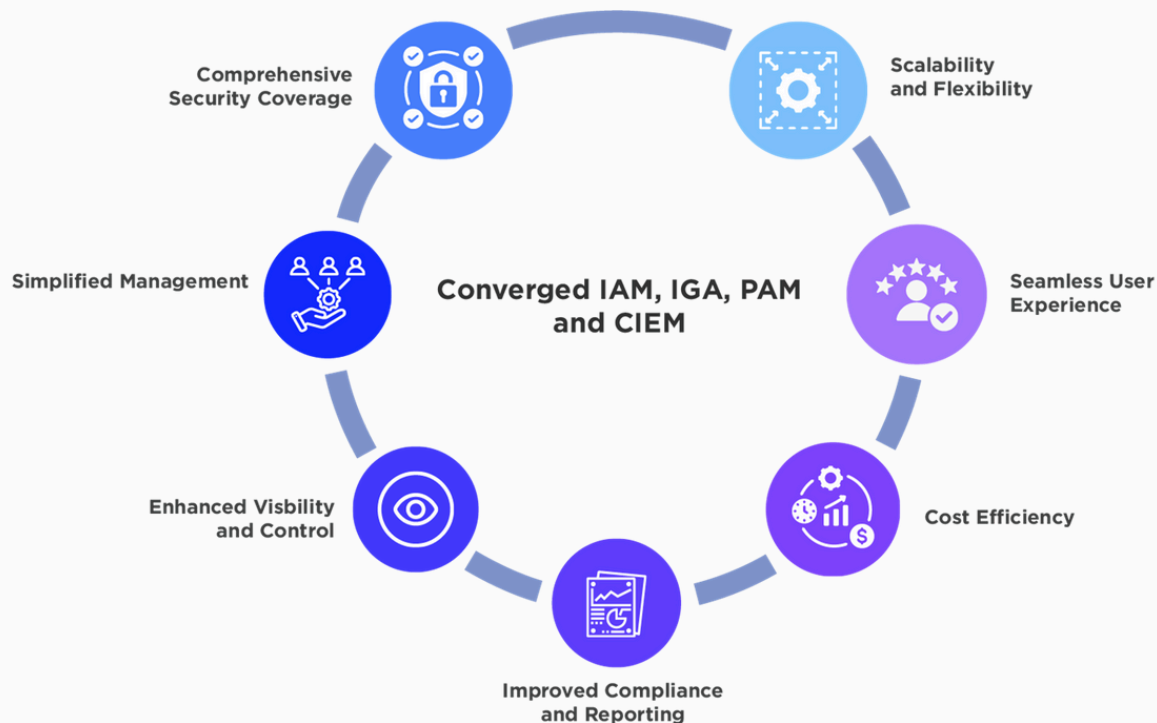
Introduction: The Identity Security Challenge

With the rise of digital transformation, businesses are adopting more applications, cloud services, and remote access mechanisms than ever before. This rapid expansion makes managing identities across various systems a growing challenge. Traditionally, identity management has been divided into three separate disciplines:

- Identity and Access Management (IAM), which handles user authentication and access to systems.
- Identity Governance and Administration (IGA), which focuses on governance, ensuring that the right users have the right access at the right time.
- Privileged Access Management (PAM), which manages, monitors, and secures privileged accounts.

Individually, these components provide value; however, the complexity of integrating and managing disparate solutions introduces inefficiencies, gaps in security, and increased administrative overhead. A converged identity platform brings these components together under a unified architecture, resulting in improved security, user experience, and operational efficiency.

The Benefits of Converged Identity Security Platform



1. Unified Visibility and Control

A converged identity platform provides a single pane of glass view for administrators, allowing them to oversee identity-related activities across all users and accounts, from regular employees to privileged administrators. By consolidating IGA, IAM, and PAM into one system, organizations can:

- Monitor access more effectively across both standard and privileged accounts.
- Identify and mitigate risks such as orphaned accounts, over-provisioned users, and unauthorized privilege escalations.
- Enforce policies uniformly across all identity layers, reducing the risk of human error.



The Benefits of Converged Identity Security Platform contd

2. Improved Security Posture

One of the primary benefits of integrating IGA, IAM, and PAM is the holistic security it provides. By breaking down silos between these components, organizations can:



- Ensure that privileged access adheres to governance rules, reducing the risk of insider threats.
- Enforce role-based access control (RBAC) consistently across all systems, ensuring that users only have the access they need.
- Automate key security processes, such as Just-in-Time (JIT) access provisioning, secrets management, and password rotation for privileged accounts, reducing the attack surface.
- A AI enabled converged platform also supports continuous monitoring, enabling real-time detection and remediation of suspicious activities, ensuring that any unauthorized access is swiftly addressed.

3. Streamlined Compliance and Auditability

Compliance with regulatory requirements (e.g., GDPR, HIPAA, SOX) is essential for modern organizations. A converged identity platform simplifies the process of demonstrating compliance by:



- Centralizing audit logs and providing clear records of who accessed what, when, and how. This unified view of access and activities across the organization reduces the complexity of audits.
- Ensuring that access to sensitive data, systems, and applications adheres to least privilege principles and meets the stringent standards required by regulations.
- Automating periodic access reviews, enabling audit readiness at all times and reducing the manual effort associated with access certifications.



4. Enhanced User Experience

A key pain point for users and administrators alike is the friction associated with managing multiple identity tools and systems. A converged identity platform offers:

- Single sign-on (SSO) capabilities across applications and systems, improving user productivity by reducing the need to manage multiple passwords.
- Self-service portals for password resets, access requests, and access reviews, empowering users to manage their own identities within a governed framework.
- Seamless integration between IGA, IAM, and PAM, allowing privileged users to request and gain access to critical resources without cumbersome delays, while ensuring that access is fully governed.



5. Operational Efficiency and Cost Reduction

Operating separate systems for IGA, IAM, and PAM not only introduces complexity but also increases costs. A unified identity platform:

- Reduces administrative overhead by automating workflows such as onboarding, offboarding, and access certifications.
- Lowers total cost of ownership (TCO) by eliminating the need for separate tools, reducing infrastructure and licensing costs.
- Simplifies the identity lifecycle by creating predefined connectors and workflows, which reduce the amount of manual intervention required from IT and security teams.



6. Scalability and Future-Readiness

As organizations scale and adopt new technologies such as cloud platforms, Internet of Things (IoT), and artificial intelligence (AI), identity needs will continue to evolve. A converged identity platform:

Is built to scale alongside the organization, supporting new users, devices, and services as needed.

Offers future-proof integration with cloud services, enabling seamless identity management across on-premises and cloud environments.

Provides robust API integration capabilities, allowing the platform to easily extend to new systems and integrate with next-generation technologies.



Use Case: Reducing the Attack Surface in a Hybrid Environment

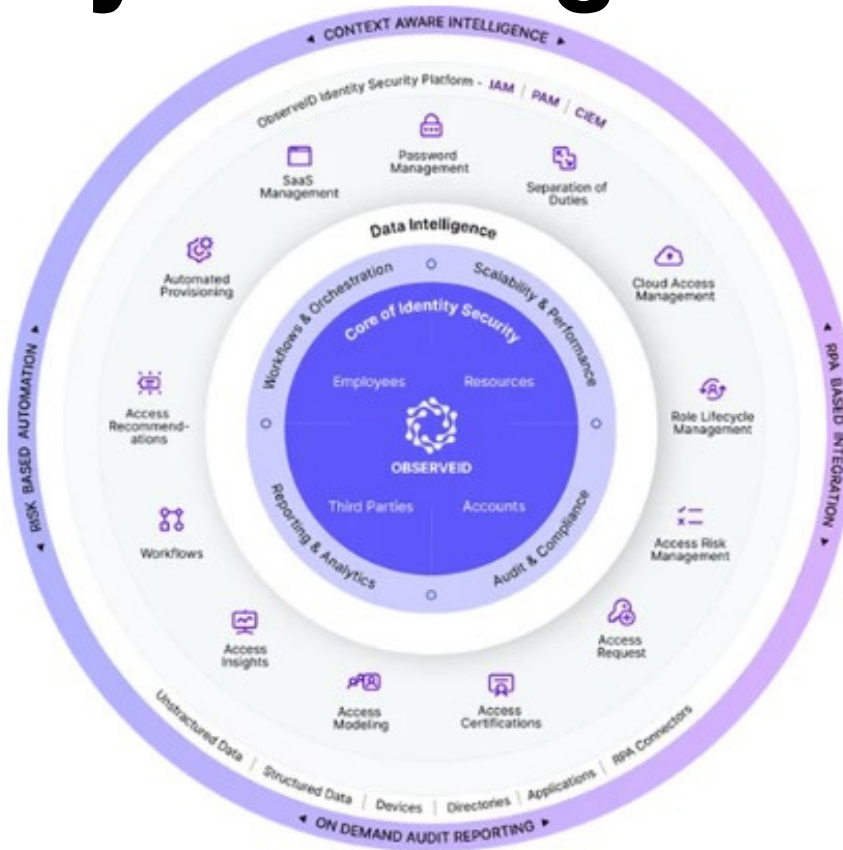
Consider an organization with multiple cloud environments (AWS, Azure, GCP), each using a different set of tools for access management and privileged account control. The lack of integration between these tools often leads to gaps in visibility, inconsistent access controls, and increased risks from compromised credentials.

By deploying a converged identity platform, the organization can:

- **Centralize** user and access management, ensuring that identities and privileges are consistently enforced across cloud environments.
- **Leverage single sign-on** (SSO) to improve user experience while strengthening security.
- **Monitor privileged access** across the entire environment, using unified policies to prevent abuse of privileged accounts.
- **Automate compliance** by maintaining a single audit trail across all clouds, simplifying reporting and reducing time spent preparing for audits.

The result is a significantly reduced attack surface, stronger security, and operational efficiency gains across the organization.

Conclusion: The Future of Identity is Converged



The traditional approach of managing IGA, IAM, and PAM as separate systems is no longer sufficient in today's complex IT environments. A converged identity platform not only provides greater security and compliance, but it also drives efficiency, scalability, and cost savings. Organizations that embrace this unified approach are better positioned to manage the growing complexity of identity in the digital age, safeguarding their critical assets while enabling their workforce.

As identity-related threats continue to rise, adopting a converged identity platform becomes not just a strategic advantage, but a necessary step in securing the future of the modern enterprise.

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. Gartner Research "Identity Governance and Administration (IGA): Understanding the Future of Identity Management" Gartner, Inc. <https://www.gartner.com>
2. Forrester Research "The Total Economic Impact™ of a Converged Identity Platform" Forrester, Inc. <https://www.forrester.com>
3. NIST Special Publication 800-63 "Digital Identity Guidelines" National Institute of Standards and Technology (NIST), U.S. Department of Commerce, <https://nvlpubs.nist.gov>
4. KuppingerCole Leadership Compass. "Leadership Compass: Identity Governance and Administration" KuppingerCole Analysts AG, <https://www.kuppingercole.com>
5. IBM Security Whitepaper, "Converged Identity: Simplifying and Strengthening Your Security Posture with IGA, IAM, and PAM Integration" IBM Corporation <https://www.ibm.com/security>
6. Identity Defined Security Alliance (IDSA) "Best Practices for Implementing Identity-Centric Security"
7. Identity Defined Security Alliance, <https://www.idsalliance.org>
8. McKinsey & Company "Securing the Cloud: The Need for a Unified Identity Management Strategy" McKinsey & Company <https://www.mckinsey.com>

Why we launched ObservelD

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?

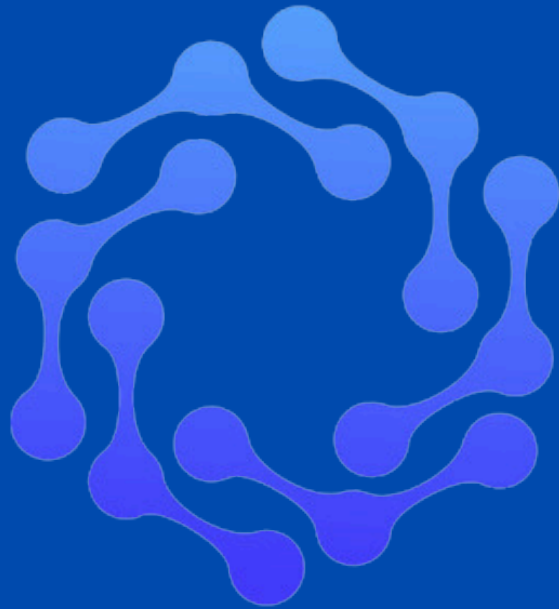
Imagine the boost in confidence for an organization when they know their data is solid, their security risk is under control, and they've got a cost-effective, agile IT infrastructure.

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

CONFIDENCE

Contact Us



ObserveID

(949)307-8116

Phone

confidence@observeid.com

Email

www.observeid.com

Website

California, USA

Address