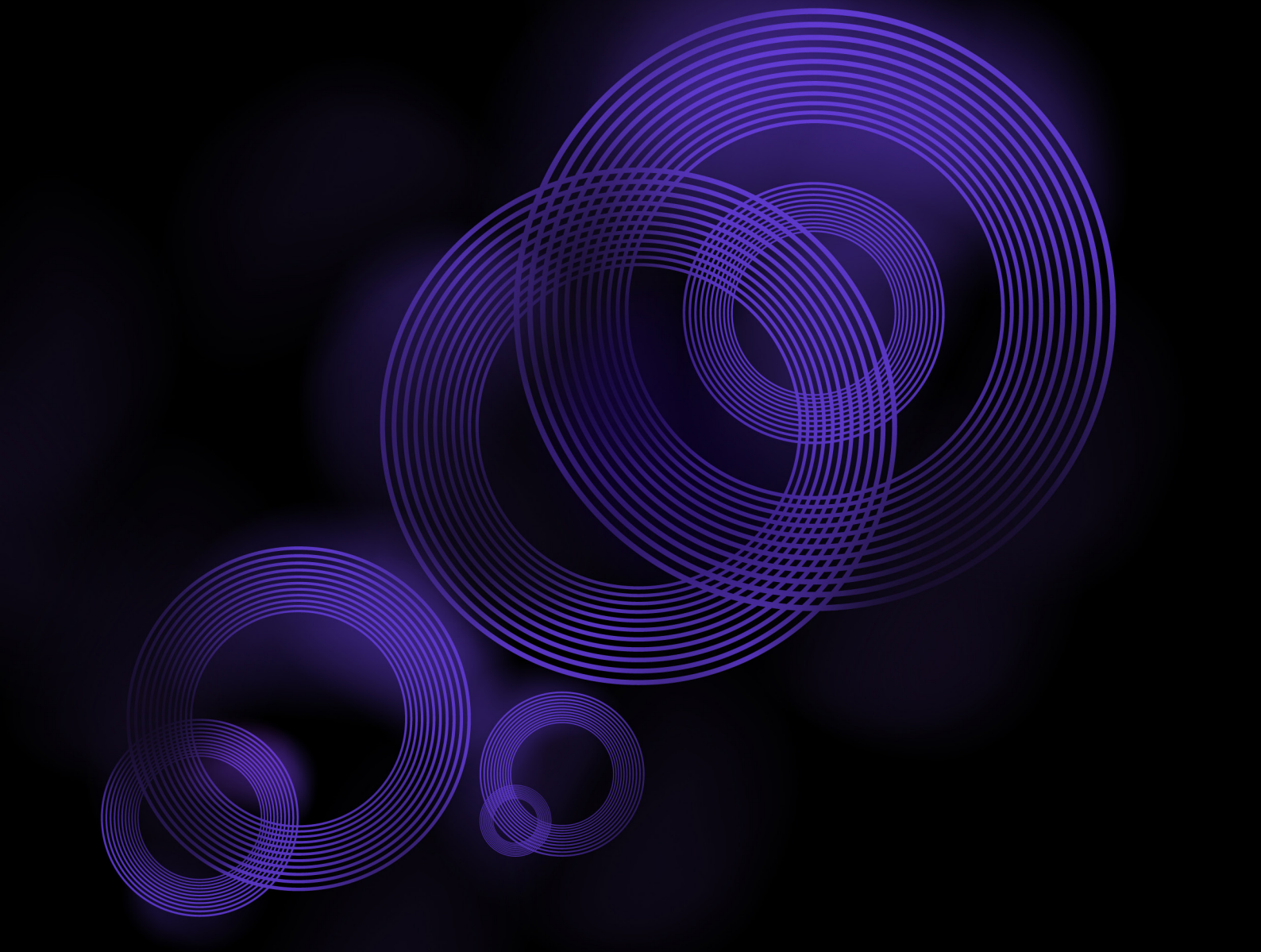
Software Analyst®
Cyber Research

MAY 2025



FROM COMPLEXITY TO CONTROL:

USING AI AND AUTOMATION TO TRANSFORM ENTERPRISE IDENTITY GOVERNANCE SECURITY

LINX Lumos cerby

About Us

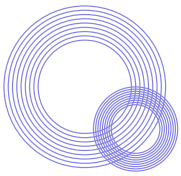
Software Analyst Cybersecurity Research (SACR) delivers in-depth analysis of the ever-evolving cybersecurity industry. Specializing in SOC, Identity, Network, Cloud, AppSec, and AI Security, our mission is to empower CISO's, security leaders, investors, and cybersecurity professionals with the knowledge they need to navigate this complex field.

Table of Contents

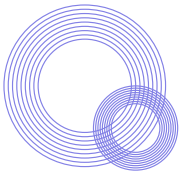
Actionable Summary

As identity becomes the new perimeter with AI, Agents, and the tremendous change happening within the enterprise, Identity Governance and Administration (IGA) is undergoing a shift from slow, compliance-heavy processes to agile, intelligent control systems. Earlier this year, **Securing the Identity Attack Surface: A Deep Dive into the New Battlefield of Identity Security,** explored some of the emerging trends within identity.

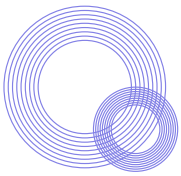
In today's report, we explore one of the largest market categories in cybersecurity. Here are some key preambles as you read this report:



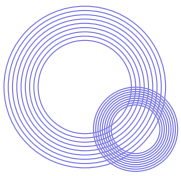
- IGA is a $50B market size driven by the convergence of identity, cloud security, and compliance requirements. The leading vendor in this market, SailPoint, was one of the first IPO companies this year. SailPoint is a $10B company approaching $1B in revenues.



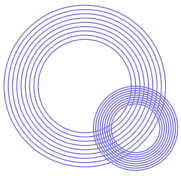
- This report provides a foundational understanding of Identity Governance and Administration (IGA), breaking down its core concepts, practical applications, and strategic importance as a critical pillar in the future of identity security. Our goal is to make this report both educational and actionable. The goal is to modernize your IGA programs and navigate the evolving identity landscape with confidence.



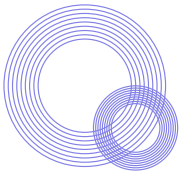
- IGA is essential because it governs who has access to what in an organization, across cloud, on-prem, and hybrid environments. As identity becomes the new security perimeter, IGA ensures that access is appropriate, compliant, and continuously reviewed.



- The most consistent IGA pain point we hear from enterprise leaders is that basic identity events like onboarding a new employee or removing access when someone leaves still rely on tickets, emails, and spreadsheets. That's not just inefficient; it's risky. There are many challenges we hear about the state of IGA.



- The SACR partnered with three unique vendors to spotlight how each is solving major pain points within the identity security ecosystem. We wrap up the report highlighting their architecture and capabilities.



- This report identifies five key areas where automation is helping enterprises not only improve security but also reduce operational friction and complexity. These insights are based on industry research, vendor capabilities, and practical experience across Fortune 500 organizations. When identity lifecycle events are automated and connected to your HR and IT systems, you not only eliminate busywork but also close critical access gaps that attackers love to exploit.

IGA Identity Market Ecosystem

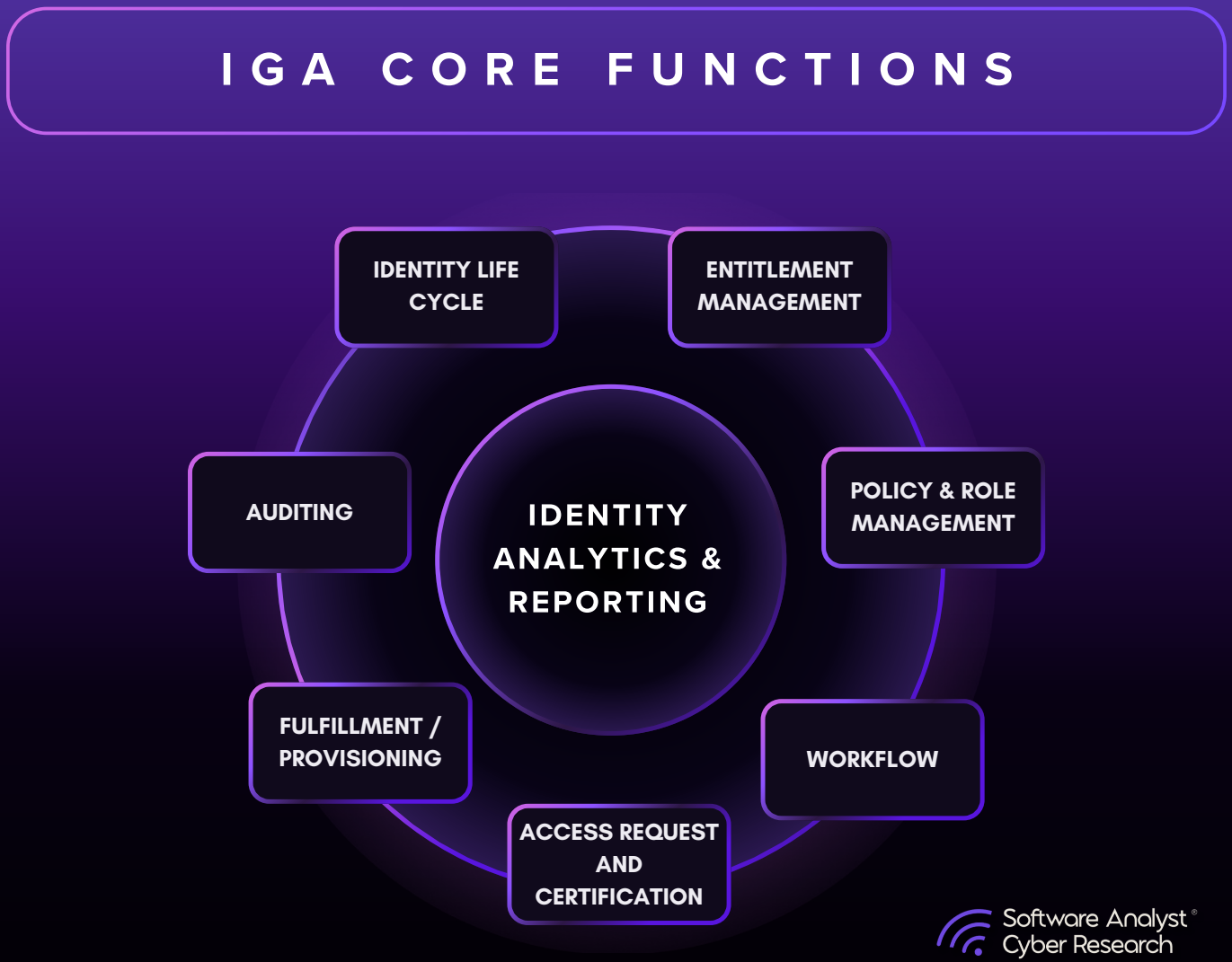
The IGA ecosystem has evolved into a dynamic and fragmented market, driven by the growing complexity of identity sprawl, cloud-first architectures, and increasing audit pressures. This market map helps decode the landscape highlighting both legacy leaders and emerging innovators that are redefining how access is governed across today's hybrid environments. From core IGA engines to adjacent platforms solving for policy automation, disconnected apps, or non-human identities, this visual provides a strategic snapshot of the players shaping the future of identity governance.

Introductory Blurb

What is Identity Governance And Access?

Identity Governance and Administration (IGA) is the discipline within identity security focused on ensuring the right individuals have the right access to the right resources at the right time, and that this access is continuously governed. IGA is both a process and a system, often implemented through platforms like SailPoint, Saviynt etc.

Put simply, IGA refers to the activities an organization must perform to make sure that all users who interact with the organization such as: employees, contractors, partners, or customers, have just the right level of access to systems and applications needed to be effective in their role, while ensuring that nobody has access they don't need or shouldn't have.

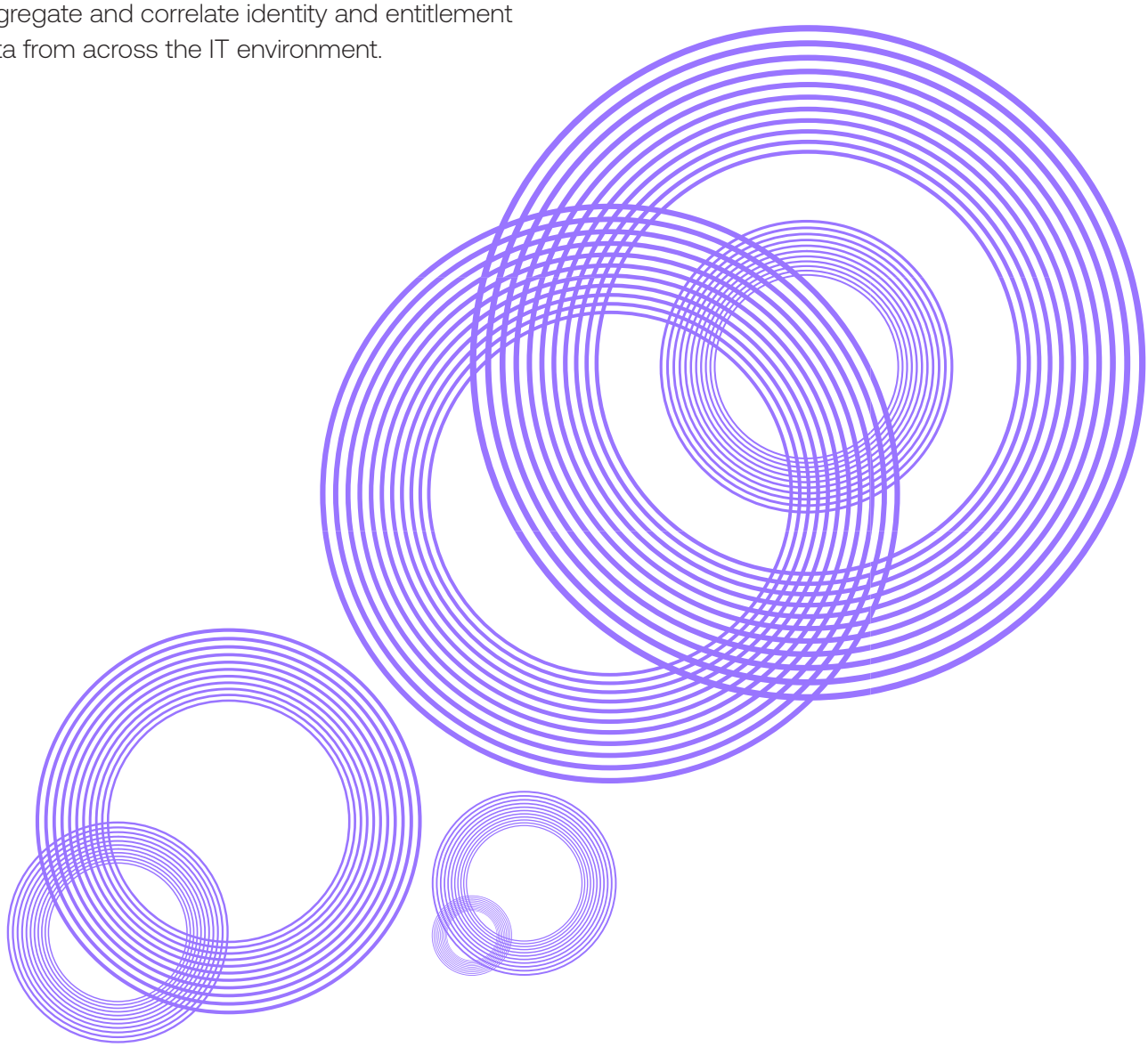


IGA vs AM/SSO

In contrast, Access Management (AM), including SSO (Single Sign-On) and MFA (Multi-Factor Authentication), is concerned with how users authenticate and gain access to systems in real time. AM enforces secure access at the point of login, while IGA ensures that the access granted is appropriate, necessary, and compliant. In short: AM controls access at the door, IGA decides who should have the key and for how long.

Additionally, it's a policy framework and a set of security solutions that enable the management of digital identities and access rights across disparate enterprise systems. These tools automate the creation, management, and certification of user accounts, roles, and access rights. They also aggregate and correlate identity and entitlement data from across the IT environment.

When implemented, IGA tools give IT administrators a comprehensive view of digital identities within their organization and streamline user provisioning, password management, policy enforcement, access governance, and access reviews. As a core component of the IAM architecture, IGA helps organizations improve process maturity, ensure regulatory compliance, and reduce the risk of unauthorized access. Key IGA functions include identity lifecycle management, entitlement management, access requests and certification, policy and role management, auditing, and identity analytics and reporting.

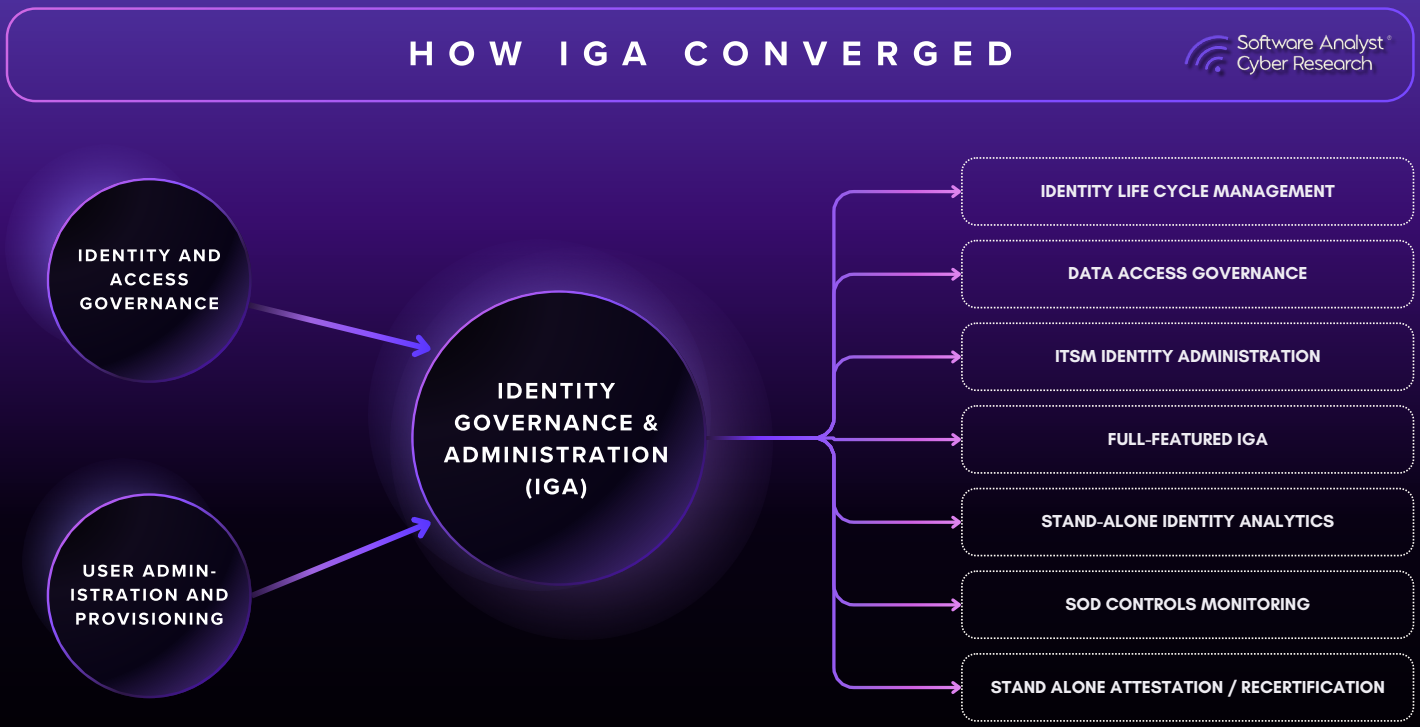


The History of IGA

The IGA market emerged a few years ago when user administration and provisioning (UAP) capabilities were gradually blended with identity and access governance (IAG) tools, a process led by IAG (SailPoint) and UAP (IBM) vendors. While most organizations have some IGA processes in place (vendor-based or home-grown manual process), IGA solutions are more commonly used by mid-sized to large enterprises These organizations benefit most from the value of mature IGA programs due to their size, complexity, and disparate systems.

Within the overall IAM suite, IGA tools have a distinct purpose: defining and enforcing IAM policies and ensuring IAM functions meet audit and compliance requirements. IGA is typically the most complex component in IAM and is often time-consuming to implement due to the need for integration, customization, and cross-departmental approvals. As a result, third-party professional services are frequently used for deployment.

The IGA market is considered mature, with limited feature differentiation between vendors. New sales are often brownfield deployments, with innovations like predictive governance and identity analytics helping to drive win rates. To stand out, vendors have expanded into adjacent areas. Saviynt, for instance, has added PAM features, while SailPoint has introduced cloud security capabilities. Cloud adoption has accelerated, offering simplified deployment and lower total cost of ownership. SaaS-delivered IAM platforms that combine access management and IGA, or PAM and IGA, are becoming increasingly popular, especially among smaller organizations with less complex IGA needs. To reduce cost, such organizations are increasingly shifting toward "IGA-light" deployments that include basic capabilities, such as segregation of duties (SOD) monitoring, identity life cycle management, and attestation/ recertification.



How IGA works

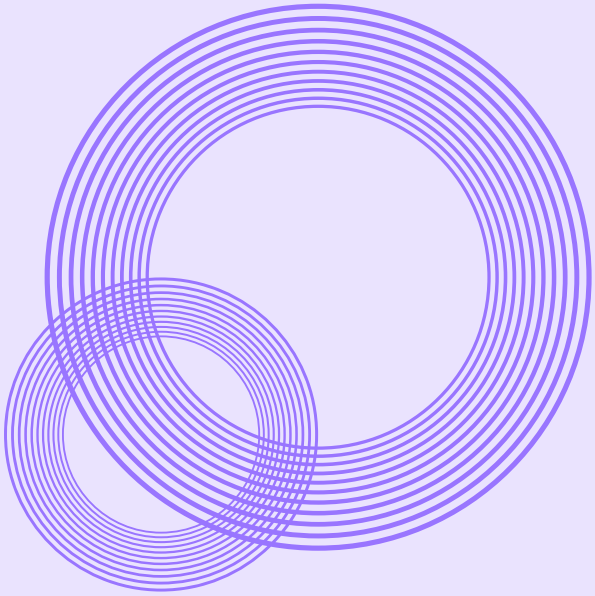
The Identity Governance and Administration (IGA) lifecycle begins with identity creation, often triggered by a new hire or contractor onboarding in an HR system. From there, IGA platforms automate the provisioning of access to appropriate systems, applications, and data based on predefined roles or attributes. As users move across departments, change roles, or take on new responsibilities, the system dynamically adjusts their access through role-based or attribute-based controls. Throughout their tenure, IGA ensures continuous governance through policy enforcement, access requests, and certification reviews—providing visibility into who has access to what, and why. When a user leaves the organization, IGA automates the deprovisioning of access across all systems, reducing the risk of orphaned accounts. At every stage, audit trails and identity analytics ensure compliance, enforce least privilege, and strengthen the overall security posture.

How IGA is Changing

IGA is undergoing a significant transformation, driven by the need to manage increasingly complex and dynamic access environments. Organizations are grappling with a surge in cloud applications, the proliferation of both human and non-human identities (NHIs), and the imperative to enforce granular access policies while maintaining agility.

Identity has replaced the network perimeter as the dominant attack surface. Modern adversaries no longer exploit firewalls; they simply obtain legitimate credentials and move laterally through over-provisioned access rights. Enterprises now juggle thousands of SaaS and cloud services and must govern both human and non-human identities in real time. Traditional IGA suites, built for slower, on-premises environments, cannot keep pace with this scale or speed, driving a shift toward automation-first, "autonomous" identity governance.

Traditional IGA solutions often struggle to address the complexities of modern IT environments, particularly the proliferation of "disconnected applications" – those lacking APIs or standard integration capabilities. This report provides an in-depth study of IGA, designed to extend the reach of IGA, with a focus on its ability to aid IGA teams and modernize identity management for these challenging applications.



The Evolving Landscape of Identity Governance

Traditional IGA solutions often struggle to keep pace with the scale and velocity of modern enterprise IT. Several factors contribute to this challenge:

1. **Explosion of Applications:** The sheer number of applications, particularly SaaS offerings, has increased exponentially. This makes it difficult for IGA teams to maintain visibility and control over access to all systems.
2. **Rise of Non-Human Identities (NHIs)**: In addition to human users, organizations must now manage a growing number of machine identities, such as service accounts, bots, and APIs. These NHIs require careful governance to prevent unauthorized access and potential security breaches.
3. **Dynamic Access Requirements**: Access needs are constantly changing due to employee onboarding, offboarding, role changes, and project-based work. IGA solutions must be able to adapt quickly to these changes to ensure that users have the right level of access at the right time.
4. **Need for Granular Policies**: Organizations need to enforce granular access policies to adhere to the principle of least privilege and comply with regulatory requirements. This requires IGA solutions to provide fine-grained control over entitlements and permissions.

Challenges Today Driving A Need For Change In IGA

Market forces are accelerating the need for automation

Three pressures make manual governance untenable. First, application sprawl has multiplied entitlement volume ten-fold, overwhelming quarterly certification campaigns. Second, the rise of contractor, bot and service account identities means provisioning and de-provisioning events now occur continuously, not in HR triggered bursts. Finally, auditors are raising the bar: defence-in-depth now demands evidence of least-privilege by default and provable access remediation within hours of a risk signal. These dynamics create demand for platforms that can discover identities, recommend policy, execute lifecycle actions and feed compliance artefacts back to control owners with minimal human intervention. Traditional, campaign-driven governance processes built around quarterly attestations and manual ticket queues no longer scale. Enterprises now require continuous controls that discover, assess, and remediate access risk with minimal human touch. These dynamics favor platforms that embed automation throughout the governance lifecycle: ingest, analyze, decide, act, rather than stopping at detection.

IGA programs are under mounting pressure from these simultaneous forces:

1. **Identity complexity**: Organizations must manage proliferating human and machine identities across workforce users, contractors, service accounts, and APIs across SaaS, on-prem, and cloud platforms. Manual spreadsheets and static role models quickly lose fidelity, leading to orphaned accounts and privilege creep. Another industry survey by Omada found that time-consuming manual processes are the #1 issue driving IGA investment, indicating that organizations are acutely feeling the pain of current manual JML handling. Furthermore, legacy IGA tools often cannot adapt easily to new cloud apps or changes, leading to extensive custom coding for connectors. Over half of organizations report that developing and maintaining custom connectors and provisioning scripts for their IGA is a significant burden.
2. **Talent scarcity**: Identity teams, SOC analysts, and application owners have limited capacity to engage with new dashboards or custom query languages. Tools must reduce operational overhead rather than add to it.
3. **Audit intensity & Regulatory oversight**: Boards and regulators increasingly require evidence that excessive privileges are detected and removed within set time frames. Security leaders must demonstrate continuous, repeatable controls rather than one-off, heroic, end-of-quarter cleanups.
4. **The IGA Conundrum: Bridging the Gap in Application Coverage:** Traditional IGA tools offer essential capabilities such as provisioning, deprovisioning, access certifications, and audit logging. These tools are instrumental in ensuring compliance, reducing risk, and managing the identity lifecycle. However, a significant limitation arises

from their dependence on APIs and standard integrations. Many applications, especially older or custom-built ones, do not possess these interfaces, leaving them outside the purview of IGA. This creates a substantial gap in application coverage, forcing organizations to rely on manual processes, spreadsheets, and custom scripts to manage access to disconnected applications. These manual methods are not only inefficient and time-consuming but also introduce security vulnerabilities and increase the risk of errors. The lack of centralized control and visibility hinders auditability and compliance efforts, exposing organizations to potential regulatory penalties and security breaches

5. **The Rapid Explosion of SaaS Applications**: The rapid expansion of SaaS applications, DevOps-style release cycles, and increasingly stringent audit mandates has outpaced the capabilities of traditional, workflow-driven IGA deployments. Large organizations now average well over 1,000 cloud and SaaS applications, yet even leading IGA suites typically provide fewer than 300 out-of-the-box connectors. This discrepancy results in a "coverage gap," where 30–50% of entitlements reside in disconnected applications that lack modern APIs. Consequently, these entitlements remain outside the governance perimeter, undermining security initiatives and forcing teams to conduct costly manual attestations.

Simultaneously, regulatory scrutiny is intensifying, with EU-level frameworks like DORA demanding continuous proof of least privilege and North American privacy statutes imposing fines for overexposed personal data. According to Omada's 2025 State of IGA survey, 31% of respondents identify "AI-driven automation of low-risk access events" as the most valuable capability for meeting these evolving obligations. Several trends are shaping the future of IGA automation:

1. **Low-/no-code connector generation**: Traditional connector factories that relied on professional-services coding are being replaced by UI recorders, AI agents, and visual wizards. These tools empower security or even line-of-business staff to capture provisioning flows without writing code. This shift significantly reduces integration timelines from months to days and extends long-tail coverage to organizations with mid-market budgets.

2. **Event-driven remediation**: As identity threats shift from human users to machine identities and ephemeral cloud workloads, batch-oriented reconciliations are becoming obsolete. The emerging trend is to leverage identity events such as new user creation, separation, or policy violations as near-real-time triggers for automated revocation or privilege reduction.

Defining Autonomous Identity Governance

Based on these challenges that we have discussed extensively, we believe Autonomous identity governance extends traditional IGA by embedding AI-powered insights and event-based execution across the governance lifecycle. It begins with comprehensive visibility into both sanctioned and shadow applications, enriching this inventory with cost and usage metrics. AI role-mining algorithms propose least-privilege baselines, which are then enforced through automated workflows. The result is identity governance that adapts to business changes in real time, reduces approval fatigue, eliminates licensing waste, and improves audit posture. Lumos' public manifesto captures the shift succinctly: visibility, control, and speed, delivered on autopilot.

Actionable Recommendations for IGA Leaders

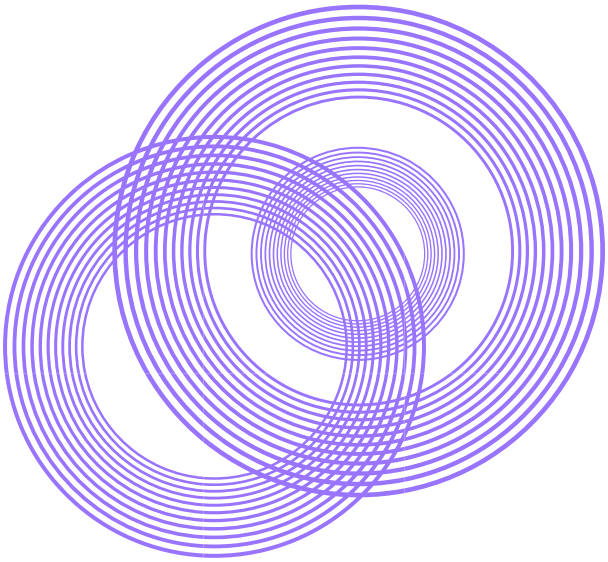
These are our recommendations for identity leaders as they think of implementing new identity programs within their enterprise.

Automate Your Identity Lifecycle Management (Streamlining Joiner–Mover–Leaver)

Challenges Today

Managing the joiner–mover–leaver (JML) lifecycle is core to IGA and one of the most error-prone when handled manually. Onboarding a new hire often involves HR entering data in one system, IT receiving a ticket, and multiple manual tasks to create access. This fragmentation leads to late Day One access, overprovisioned accounts, and lingering credentials after offboarding, posing major security risks.

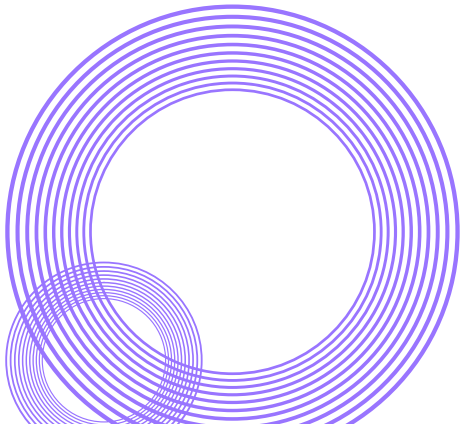
A recent survey found that fewer than 1 in 10 companies have automated app provisioning for onboarding - over 80% still rely on unstructured manual tools like emails and spreadsheets to manage user access during onboarding. Just 9% have automated provisioning. Over 60% cite manual JML as a top pain point, and 46% admit they lack automation to ensure appropriate access across systems. This manual status quo leads to frustrated employees (who wait for access) and overwhelmed IT staff dealing with backlogs of access requests and cleanup.



Our Proposed Solution

1. Start by integrating HR as the authoritative source for identity changes, then automate provisioning through connectors (e.g., SCIM). Trigger events like a new hire or termination can launch workflows that update AD, email, and business apps.
2. Pair IGA with ITSM tools like ServiceNow for broader orchestration—automating not just account access, but also badge and device recovery. Modern platforms offer low-code workflows to handle approvals, notifications, and syncs across systems.
3. For Movers, dynamic role-based provisioning ensures users don't accumulate privileges across departments. The "hub-and-spoke" model centralizes the IGA platform as the control point between HR systems, directories, and applications.

JML automation cuts manual workload by up to 70%, ensures Day One productivity, and allows near-instant deprovisioning which is critical for security. It also creates a complete audit trail for compliance and eliminates delays and errors caused by ticket-based provisioning.



Role-Based and Attribute-Based Access Control (RBAC & ABAC)

Challenges Today

Based on our work, defining "who gets what" access is fundamental but RBAC often results in role explosion or drift as businesses scale. Static roles don't adapt well to changing org structures, and users accumulate access as they switch jobs. ABAC offers dynamic control but requires clean, governed data and well-defined rules.

The absence of structured access controls leads to overprovisioned users, costly reviews, and ad-hoc entitlement grants. 70% of organizations admit to excess access, and nearly half struggle to enforce least privilege effectively.

Our Proposed Solution

1. We recommend using AI to mine existing access data and generate roles from real-world patterns. Tools can suggest common entitlements and automate assignments based on attributes like department and title.
2. Dynamic role assignment ensures users receive and lose access automatically when attributes change. For ABAC, deploy a central policy engine to evaluate contextual factors, such as location, employment status, or contract end date during access decisions.
3. Pair ABAC with Just-In-Time access to enforce tight, temporary access windows based on real-time validation (e.g., MFA). Automate remediation when attributes change, revoking access no longer justified.

When automation drives both role definition and enforcement, teams reduce manual effort, streamline provisioning, and tighten access control. Centralized rules help eliminate privilege creep and support confident, low-friction user access, boosting both security and operational efficiency.

Leverage AI for Intelligent Identity Insights and Risk-Based Access Reviews

Challenges Today

Enterprises are flooded with identity and access data. Yet most access reviews are still manual, spreadsheet-based, and lack context, leading to rubber-stamping rather than meaningful validation. Managers are expected to review long lists of entitlements with no insight into usage, risk, or anomalies.

The results? Inconsistent oversight and unnecessary access lingering across systems. Over 70% of IT leaders say users have more access than needed (Omada State of IGA 2025). Worse, 88–95% of breaches still stem from human error, like overlooking a toxic access combination or forgetting to revoke permissions.

Our Proposed Solution

1. This is where AI shines. By analyzing access patterns, peer groups, and usage behavior, AI-powered IGA platforms can spot risky access and suggest precise remediation. They score entitlements based on risk, detect outliers, and recommend appropriate access based on a user's role and activity.
2. During access reviews, automation delivers rich context, such as when an entitlement was last used, whether it violates policy (e.g., segregation of duties), and how it compares to peers. That lets reviewers focus on true risks, not rubber-stamp everything.

3. AI also enables continuous, risk-based reviews. Rather than waiting for quarterly certifications, reviews can trigger automatically based on risk thresholds, like when a user's access changes suddenly, or a dormant account becomes active. SailPoint and others visualize these identity relationships using AI-powered graphs, helping teams spot and act on outliers quickly.

By shifting from static reviews to continuous, intelligent oversight, organizations reclaim control. Managers get clarity, not chaos. Security teams can cut audit prep time by up to 90% (Saviyant,2025), as GE HealthCare reported after implementing AI-driven identity analytics.

The end state is not just compliance, it's proactive governance. AI highlights the handful of critical risks from thousands of entitlements, allowing teams to act before an incident occurs. With ML-assisted decisions and automated evidence trails, enterprises turn a historically reactive process into one that's efficient, dynamic, and audit-ready.

Extend Governance to All Applications and Consolidate Identity Sources

Challenges Today

Most enterprises run hundreds, sometimes thousands of applications. But not all apps are created equal. Legacy on-prem systems and niche SaaS tools often lack APIs or standard connectors, making them invisible to identity governance systems. This leaves significant blind spots. In fact, 58% of enterprises say their current tools cover less than half of their applications. Many IGA deployments only manage AD and a few cloud apps, leaving the "long tail" of disconnected systems unmanaged. These gaps mean orphaned accounts, inconsistent access controls, and compliance risk.

Add to this: identity data silos. M&A activity and organic sprawl leave companies with multiple HR systems, directories, and identity stores. Without consolidation, a single person may have multiple unlinked accounts. You can't enforce least privilege or run complete reviews without a unified identity view.

Our Proposed Solution

1. To address this, leading IGA vendors now offer integration brokers i.e.tools that simulate connectivity using robotic process automation (RPA) or scripting. Solutions like Cerby, for instance, allow governance for apps without APIs by automating UI actions and syncing access with central platforms
2. At the same time, IGA platforms increasingly provide flexible connectors: SCIM for cloud apps, JDBC for databases, LDAP for directories, and CSV-based sync for older systems. Enterprises should prioritize tools with broad connector libraries and the ability to configure or extend integrations easily.
3. For identity consolidation, automation helps correlate data across sources, matching users via email, employee ID, or other attributes to build a master identity record. Middleware layers (or "identity fabrics") normalize incoming data and ensure changes are reflected across all systems in real-time.

With these automation layers in place, enterprises can govern 90%+ of their app landscape, not just the obvious ones. They also gain a complete view of each identity, enabling precise policy enforcement, consistent deprovisioning, and comprehensive audit readiness.

Disconnected apps no longer remain in the shadows. Instead of fragmented account management, IT runs a single orchestrated platform. Users benefit from consistent access. Auditors see full coverage. And security teams close one of the biggest gaps in modern identity governance.


Lumos

Lumos

Lumos is a San Francisco based identity security company founded in 2020 by Andrej Safundzic (CEO), Leo Mehr, and Alan Flores-López. The company is backed by investors such as a16z and Scale Venture Partners.

Their solution provides capabilities in:

- Identity Governance and Administration (IGA): Access Reviews and Lifecycle Management
- Identity Security Posture Management (ISPM)
- Least-Privilege Access Controls
- Access Requests and Just-In-Time Access
- SaaS Discovery; Spend Optimization and Zero-Touch IT

This report analyzes Lumos, a platform designed to help IGA teams navigate modern challenges by automating key IGA functions and enabling autonomous identity governance.

How Lumos Helps IGA Teams

Lumos addresses these challenges with a modern, automated approach to IGA, offering several key capabilities that empower IGA teams to manage identity more effectively:

1. **Comprehensive Visibility:** Lumos integrates with various systems, including HRIS, IDPs, and applications, to provide a holistic view of access across the enterprise. This visibility extends to both sanctioned and unsanctioned applications, enabling IGA teams to identify and mitigate shadow IT risks. Lumos also provides detailed information about account status, login activity, and granular entitlements.
2. **Automation of Workflows:** Lumos automates key IGA workflows such as access requests, provisioning, and deprovisioning. This automation reduces manual effort, improves efficiency, and accelerates access-related processes. It also includes inactivity workflows that proactively identify and alert users or application owners about unused entitlements, helping to curb access sprawl.
3. **AI-Powered Access Reviews:** Lumos leverages AI to enhance access review processes. Its AI-powered capabilities enable the generation of access profiles and policies based on role mining, making access reviews more efficient and accurate. It also incorporates Albus, an AI agent that facilitates dynamic access decisions based on contextual information.
4. **Policy Automation:** Lumos automates the creation, refinement, and enforcement of granular access policies. By analyzing access patterns and user behavior, it can recommend and implement policies that adhere to the principle of least privilege, reducing risk and ensuring compliance.
5. **Lifecycle Automation:** Lumos automates the entire identity lifecycle, from onboarding to offboarding. This includes provisioning access for new employees, modifying access based on role changes, and revoking access when employees leave the organization. This ensures appropriate access throughout each employee's tenure.

Lumos' Autonomous Identity Governance Use Cases

In April 2025, Lumos introduced an AI-driven upgrade called the Autonomous Identity Platform. This release added the "Albus" agent, which provides on-demand connector and access policy creation, continuous policy learning that refines least-privilege controls based on evolving usage patterns, and lifecycle automation for near real-time provisioning and deprovisioning of joiners, movers, and leavers. These capabilities aim to reduce deployment times by up to sevenfold and lower the total cost of ownership compared to legacy IGA suites, while also providing security teams with streaming evidence for compliance.

Designed as the company's flagship offering, the Autonomous Identity Platform unifies SaaS management, identity governance, and privileged-access management within a single cloud service.

At its core, Lumos automatically discovers all human and non-human identities, maps entitlements across more than 300 cloud and on-premises systems, and maintains a real-time "access graph" enriched with cost and usage telemetry. Its self-service AppStore allows employees to request or revoke access via Slack or Microsoft Teams, while built-in license analytics highlight unused seats and redundant subscriptions.

Lumos' autonomous identity model leverages AI to bring a new level of automation and intelligence to IGA. These capabilities include:

1. **Autonomous policy management:** Lumos enables organizations to automate the development of access policies, reducing drift, tightening security, and minimizing compliance burden. By combining traditional machine learning with agentic AI workflows, Lumos analyzes access patterns, user entitlements, and organizational context to create, refine, recommend, and evolve role-based access controls.(RBAC).
2. **Automatically create and refine access policies:** Lumos continuously analyzes access patterns and user behavior to generate and refine access policies, ensuring alignment with business needs and security best practices.
3. **Enforce granular access policies:** Lumos enables organizations to enforce fine-grained control over entitlements and permissions, ensuring that users have only the necessary access. This helps organizations enforce the principle of least privilege, reduce access sprawl, prevent unauthorized access, and improve overall security.
4. **Make dynamic access decisions:**The Albus agent makes real-time access decisions based on contextual information such as location, time, and device, enabling adaptive access controls responsive to changing risk conditions.
5. **Automate identity lifecycle management:** Lumos automates key identity lifecycle processes and supports dynamic access controls, reducing manual effort and improving efficiency. This automation streamlines IGA workflows, freeing up IGA teams to shift focus to strategic priorities and reduces labor and audit costs.

Analyst Perspective and Conclusion

This report has discussed the role of automation within IGA projects. We believe that Lumos' new "Autonomous Identity Platform" stands out by merging AI-generated policy management with near-real-time joiner, mover, and leaver automation. Albus can generate new connectors, integrations, and access policies on demand. If it proves reliable, this could drastically reduce the professional-services backlog that haunts traditional IGA rollouts.

The Albus agent drafts RBAC rules and explains its reasoning, giving mid-size, cloud-first enterprises a faster and lighter alternative to traditional SailPoint-style implementations. By embedding approval workflows in Slack and Teams and enriching its access graph with license and cost data, Lumos connects security, IT, and finance goals in a way most incumbents do not.

The "autonomous" promise, however, hinges on proof that AI-written connectors remain stable as downstream SaaS UIs and APIs evolve, and that every policy decision can withstand audit scrutiny. Lumos must also address current gaps in large-scale segregation-of-duties analytics, service account credential vaulting, and full support for mission-critical on-prem ERP and database systems to compete directly with full-stack IGA and PAM suites.

If Lumos can deliver reliable, self-healing integrations and maintain strong ecosystem partnerships before larger vendors mature their own AI agents, it could become a durable agility layer atop existing identity platforms or replace legacy vendors altogether.

Lumos represents a new generation of IGA solutions that leverage AI and automation to address the challenges of modern identity governance. As organizations continue to grapple with increasingly complex IT environments, solutions like Lumos will be crucial for achieving effective and efficient identity governance.

Additional Recommendations for IGA Leaders

1. **Audit your IGA coverage gap**: Assess the number and criticality of applications and identities outside your current IGA scope, to understand where coverage ends and risk begins. Use this baseline to project the risk reduction and ROI of identity automation tools designed for long-tail applications. If your organization requires expanded IGA coverage and accelerated application onboarding, solutions like Cerby can help. This will improve security posture, strengthen ongoing compliance, and reduce operational overhead.

2. **Insist on event hooks:** When evaluating add-on solutions, prioritize those that can both consume and emit events, enabling near-real-time flow of revocations and certification data rather than relying on daily polls.

3. **Plan for Connector Resilience and Vendor Exit:** Mandate continuous monitoring of connector health, self-healing logic, and clearly defined SLAs. Include contractual clauses for source-code escrow or API-level export to prevent lock-in if a specialist automation vendor is acquired or sunsets a feature.

4. **Layer and extend automation:** Adopt a tiered strategy combining a core IGA engine for policy logic, Cerby-style AI agents for application and automation reach, and AI analytics for continuous role optimization. This approach delivers faster results than a complete platform replacement.

5. **Pilot AI role mining early:** Even limited deployments of AI role mining can reveal redundant access and streamline future certifications, freeing up budget for expanding integration scope.

Conclusion

Identity Governance and Administration (IGA) has long been seen as an important compliance obligation, but often burdensome. But the world has changed. In today's environment, where identities outnumber employees, access needs change by the hour, and attackers exploit privilege as their primary weapon, IGA isn't just a checkbox anymore. It's a critical business control. And more importantly, when done right, it becomes a strategic advantage.

This report has laid out a blueprint for how to transform your IGA program—from a manually intensive, slow-moving process into an automated, intelligent, and adaptive engine for security and compliance. We explored five key areas where complexity and inefficiency reign: identity lifecycle management, access reviews, role and policy enforcement, disconnected application coverage, and identity data consolidation. Each of these areas represents not just a problem, but an opportunity for automation.

The lesson across all of them is clear: manual doesn't scale, but automation does. Whether it's orchestrating joiner-mover-leaver workflows, using AI to surface high-risk access, dynamically enforcing policy through ABAC, or extending governance to shadow applications, there are now modern solutions that go far beyond what traditional IGA platforms were designed to do.

Modern IGA is not about reinventing the wheel. It's about putting that wheel on autopilot. It's about shifting from reactive cleanup to proactive control. It's about integrating insights, decisions, and actions into a continuous, data-driven feedback loop. And it's about empowering security teams to govern at the speed and scale the business demands without burning out staff or ballooning professional services budgets.

Software Analyst®
Cyber Research

https://softwareanalyst.substack.com/

https://www.linkedin.com/company/software-analyst/

https://www.linkedin.com/in/francis-odum-0a8673100/

https://x.com/InvestiAnalyst

softwareanalyst.io