Deloitte.

Together makes progress

How Agentic AI is redefining software entitlement, provisioning and access management

Transforming from compliance to revenue-shaping capability

Contents

Introduction

Software companies are moving from subscription to consumption to AI-enabled outcome-based monetization models. As everything-as-a service (XaaS) adoption accelerates—the global subscription economy market size is projected to reach $1.5 trillion by 2033[1]—traditional identity and access management (IAM), licensing, and provisioning processes are becoming strategic bottlenecks. Historically, these processes have often relied on manual, fragmented, and highly customized workflows for user identity verification, account access provisioning, and license allocations. These methods can result in operational inefficiencies, increased administrative overhead, heightened security risks, compliance breaches, and potential revenue leakage.

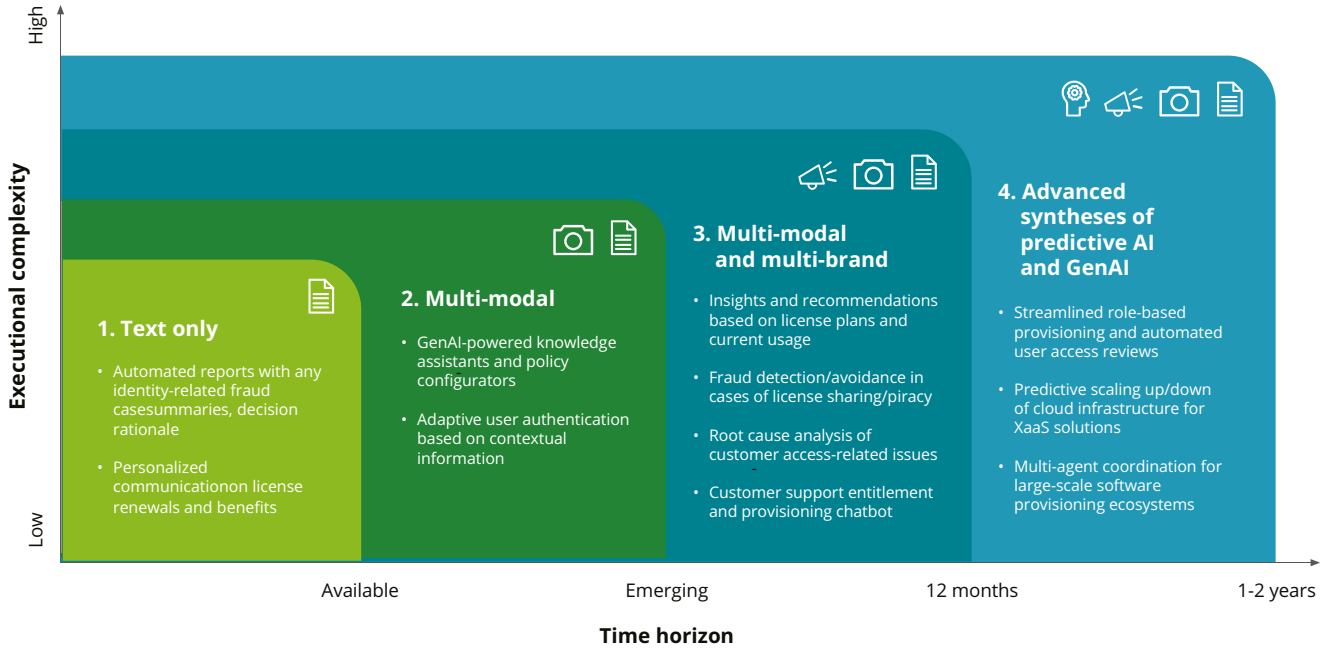
Enter agentic artificial intelligence (AI), the next evolution of Generative AI (GenAI), where intelligent agents don't just automate tasks; they can continuously govern access, licensing, entitlements, and provisioning in real time. AI-driven licensing and identity models are now capable of self-adjusting to context, recognizing who should have access, under what terms, and at what commercial moment.

Through AI agents, users and administrators can self-serve common IAM tasks, such as requesting, approving, or revoking access, thereby reducing manual effort. For enterprise partners, AI can streamline role-based provisioning, automate access reviews, and provide actionable insights into usage patterns and access anomalies. These enhancements can reduce friction and enable scalability across digital ecosystems.

Integrating AI with cloud-based platforms can help ensure that licensing models are adaptive and scalable, responding to evolving market demands and customer usage patterns. Companies leveraging AI-driven predictive analytics can forecast license demand, optimize resource allocation, and dynamically adjust contract terms based on real-time data, fostering a more agile and customer-centric approach.

The graphic below highlights AI use cases at different maturity levels.

Role of GenAI in IAM, software licensing, and provisioning



Licensing to provisioning use cases

Adaptive authentication
Technology companies frequently operate within multi-vendor ecosystems and maintain multiple in-house legacy systems and infrastructure, often leading to siloed IAM systems. These systems typically rely on static authentication methods, which require frequent manual intervention and updates to predefined rules and policies. Inadequate access control reviews can expose organizations to heightened risks of identity theft and unauthorized access due to compromised credentials. This fragmentation can make it challenging for organizations to standardize security policies and effectively protect user identities.

By leveraging AI-driven adaptive authentication, organizations can dynamically adjust the user authentication requirements based on location, device usage patterns, login time, behavior, and other contextual factors. AI can assess the risk to login attempts in real time, detect potential anomalies, and determine the need for additional authentication steps using contextual information. By analyzing vast data sets, AI can prompt users for re-authentication, initiate additional authentication steps, or flag suspicious behavior.

Potential benefits include:

Operational efficiency/cost savings

- Increased cost savings by mitigating identity-based attacks, preventing data breaches, and safeguarding sensitive customer data
- Improved compliance and regulatory adherence through proactively blocking fraudulent attempts and unauthorized access

Customer experience

- Improved customer trust through robust security measures
- Streamlined customer login experience with adaptive authentication
- Greater customer peace of mind and understanding about how AI safeguards their digital identities

Employee experience

- Reduced manual intervention through automated adjustments of authentication requirements based on contextual information

Intelligent access control policies

Managing access control policies is a growing challenge as organizations face increasing complexity from hybrid IT environments and decentralized systems. These challenges are compounded by the dynamic nature of modern application environments, which demand context-aware, risk-sensitive, and policy-driven access controls that can adapt to evolving business needs and threats. Traditional identity governance models lack consistent enforcement of access policies across diverse systems, which can lead to misconfigurations and elevated risk of unauthorized access. Additionally, they struggle to provide real-time visibility into who has access to what, in which systems, and under what conditions—limiting the organization's ability to detect and respond to access-related risks effectively.

By analyzing large volumes of identity and activity data, AI can assist IAM teams in dynamically modeling access roles and recommending tailored policies that align with business functions and risk thresholds. Through conversational assistants, AI can also simplify the creation, evaluation, and tuning of access control policies, making IAM operations more accessible. Furthermore, with mechanisms like retrieval-augmented generation (RAG), AI systems can ensure that access recommendations are based on up-to-date, authorized enterprise data, improving policy accuracy while reducing administrative overhead.

Potential benefits include:

Revenue growth

- Improved compliance and regulatory adherence through proactively blocking fraudulent attempts and unauthorized access

Operational efficiency/cost savings

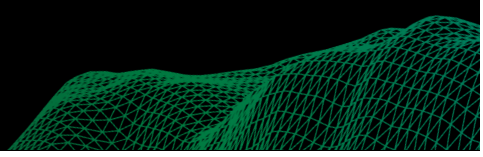
- Decreased audit and compliance overhead with interactive, visual analysis of access patterns and risks
- Streamlined access approvals and exception handling through AI-generated policy recommendations

Customer experience

- Reduced access errors and delays through AI-assisted policy evaluations that ensure customers are granted the right access at the right time
- Enhanced trust and usability by enabling intelligent, policy-driven access decisions that adapt in real time to customer context (e.g., device, location, behavior)

Employee experience

- Improved IAM administrator productivity with conversational tools that simplify the authoring, tuning, and simulation of complex access control policies
- Reduced manual IAM workload and policy administration through automated insights and AI-driven access control optimization



Role-based access control (RBAC) optimization

Software-as-a-service (SaaS)-based businesses have fluctuating needs and user roles, which can result in complex and time-consuming processes to manage user access controls. Ensuring users have appropriate access based on their roles and applying policies consistently across the organization typically involves a lot of manual effort. Any potential oversight due to manual effort can result in security gaps or misuse of sensitive information.

Many leading providers use AI to continuously monitor access logs and user activities based on user roles and dynamically adjust access controls in real time. AI analyzes the existing access control policies and recommends optimizations to speed up the process of granting/revoking user access. For example, in some organizations, access provisioning is based on legacy reporting structures such as when a new hire inherits all the access rights of a long-serving manager who has rotated through multiple roles. AI identifies such mismatches, recommends corrections, revokes the incorrect access, and grants the correct permissions. It can also provide insights and recommendations to refine roles and permissions to better match actual usage patterns. This can ensure scalability without compromising on user experience or security breaches.

Potential benefits include:

Revenue growth

- Ability to handle more users and roles as the business scales without compromising performance and security
- Enhanced protection of organizational data and resources and improved compliance with evolving regulatory requirements

Operational efficiency/cost savings

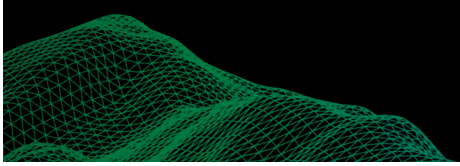
- Dynamically adjusted access permissions based on role changes without manual intervention
- Increased cost savings through reduced need for administrative overhead through automation of RBAC

Customer experience

- Tailored access based on user's needs and roles through adaptive access controls
- Expedited user onboarding through quick and efficient RBAC assignment

Employee experience

- Fewer access-related issues and reduced time spent on troubleshooting
- Reduced administrative overhead from lengthy manual approval process



Identity verification and fraud detection

Organizations face mounting challenges in verifying digital identities and detecting fraud across increasingly complex and high-volume user interactions. The rapid rise in account takeover attempts, synthetic identity creation, and deep-fake-enabled fraud has exposed weaknesses in traditional credentialing, authentication, and account recovery workflows. Compounding the issue is the use of fragmented identity and fraud management tools, which often operate in silos, limiting visibility into user behavior patterns, risk signals, and cross-channel anomalies—ultimately slowing response times and increasing exposure to fraud.

AI can help transform identity verification and fraud detection by powering intelligent, context-rich decision-making at scale. It can enable real-time evaluation of biometric signals and behavioral patterns by synthesizing structured and unstructured data across diverse identity sources. For fraud detection, AI can enhance anomaly detection models, generating synthetic fraud scenarios for training and fraud investigators triaging alerts, surfacing insights, and explaining risk scores. In account recovery, conversational AI interfaces guide users through secure workflows, helping improve both UX and accuracy.

Potential benefits include:

Revenue growth

- Scaled growth of high-trust digital interactions by ensuring secure access to services across geographies and customer segments
- Accelerated market expansion by aligning identity verification with regional compliance and fraud prevention needs

Operational efficiency/cost savings

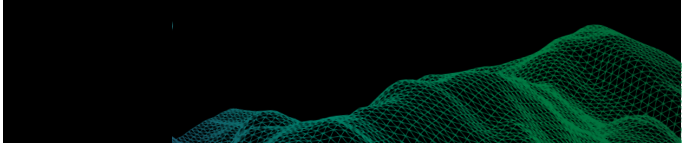
- Reduced fraud-related revenue loss by detecting and preventing account takeovers and synthetic identities
- Fewer false positives and verification retries by using adaptive, risk-aware verification paths

Customer experience

- Improved account recovery through natural language guidance and AI-orchestrated workflows tailored to user context and risk level
- Strengthened digital trust by providing transparent, explainable identity verification decisions and accelerating resolution

Employee experience

- Enhanced productivity with AI-generated case summaries, decision rationale, and reports
- Faster learning curve for fraud and IAM teams with AI-powered knowledge assistants and policy configurators



Automated and predictive software license analysis

XaaS-based businesses have complex licensing models that vary by user, device type, and features. As business scales, managing and analyzing an increasing number of licenses becomes cumbersome and resource-intensive, making it hard for organizations to address specific business needs and licensing requirements. Additionally, a lack of centralized license tracking mechanism can often result in inefficiencies such as underutilized licenses and overlapping subscriptions.

AI can analyze license usage data to help organizations better forecast future needs by gaining insights into underutilized or overutilized features and identifying factors that influence license renewal rates. By analyzing customer profiles, usage patterns and preferences, historical license renewal data, and changes in subscription plans, AI can help organizations make decisions based on data-driven insights. It can also provide recommendations such as upgrading to a higher tier in cases of overutilized licenses, reallocating underutilized licenses or adjusting subscription plans based on usage patterns.

These capabilities complement, rather than replace, established software asset management (SAM) tools. One of AI's strengths lies in predictive forecasting and conversational interfaces that can help executives and employees understand license usage without deep technical expertise.

Potential benefits include:

Revenue growth

- Improved opportunities to up-sell or cross-sell additional licenses by analyzing based on license renewal patterns and customer usage data
- Increased volume of renewals through proactive engagement of at-risk customers based on insights from predictive analysis of license renewal patterns
- Support for growth and scalability through accurate license requirements forecasting

Operational efficiency/cost savings

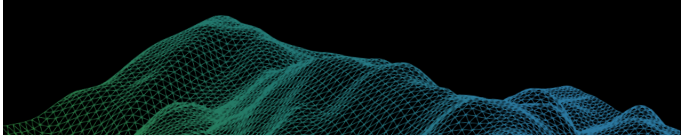
- Reduced costs through better license allocation and usage, with increased visibility into usage trends
- Reduced revenue leakage from better asset management and timely license renewals
- Decreased churn rates through more targeted and personalized customer engagement

Customer experience

- Improved customer experience through proactive communication including automated reminders and personalized communications
- Real-time support for renewal-related queries with accurate assistance for complex/specific customer concerns

Employee experience

- Increased employee productivity and performance through automation of repetitive tasks, access to real-time data and insights, and improved decision-making
- Improved decision-making through predictive insights into future license requirements for optimizing license renewals, re-allocation, or termination



Dynamic entitlement provisioning

XaaS-based businesses often manage various licensing models that can make scaling services up/down time-consuming and complex. It can lead to customer dissatisfaction due to delayed access provisioning or revenue leakage in cases where customers are able to access services without having paid for it due to incorrect provisioning. If the entitlement systems are rigid and lack the flexibility to provide real-time data insights on customer usage patterns, it can be difficult for organizations to optimize the services. Leveraging AI can help organizations dynamically adjust entitlements including controlling and adjusting user access rights and provisions by analyzing contractual data, access patterns, and under/over licensing utilization. AI can be used to predict future access needs and continuously adjust policies based on changes in user roles, organizational policies, and security assignments to ensure optimal level of provisioning.

Potential benefits include:

Revenue growth

- Improved ability to quickly scale services through real-time adjustment to entitlements based on customer contracts and usage patterns
- Optimized service offering through data-driven decision-making facilitated by real-time insights into customer usage and entitlements

Operational efficiency/cost savings

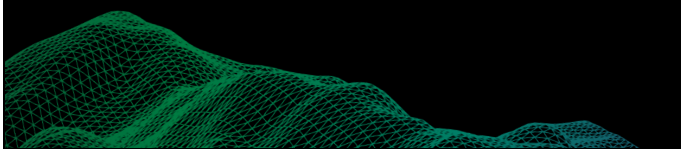
- Automated user access reviews and provisioning based on customer entitlements

Customer experience

- Improved customer experience through automated and accurate entitlement provisioning

Employee experience

- Reduced administrative overhead and decreased effort required to manage user accounts through automated and streamlined provisioning process
- Minimized errors/incorrect provisioning due to manual processes



The future of licensing to provisioning function

The next phase of XaaS IAM, licensing, entitlement, and provisioning will not be defined by efficiency alone. It will likely be defined by autonomy, auditability, and assurance—delivered through agentic AI solutions that act as trusted intermediaries between business intent and user action.

Those that move early could gain the intelligence advantage—transforming what used to be a compliance function into a predictive, revenue-shaping capability.

Contacts

Jagjeet Gill
Principal
Strategy
Deloitte Consulting LLP
jagjgill@deloitte.com

Ravleen Chawla
Senior Manager
Artificial Intelligence & Engineering
Deloitte Consulting LLP
rchawla@deloitte.com

Ani Karapetyan
Senior Consultant
Strategy & Transactions
Deloitte Consulting LLP
akarapetyan@deloitte.com

Key contributers

Mike Vehlewald and Sean Tice

Endnotes

1. Grand View Research, *Subscription economy market (2025–2033)*, accessed December 2025.

Deloitte.

Together makes progress