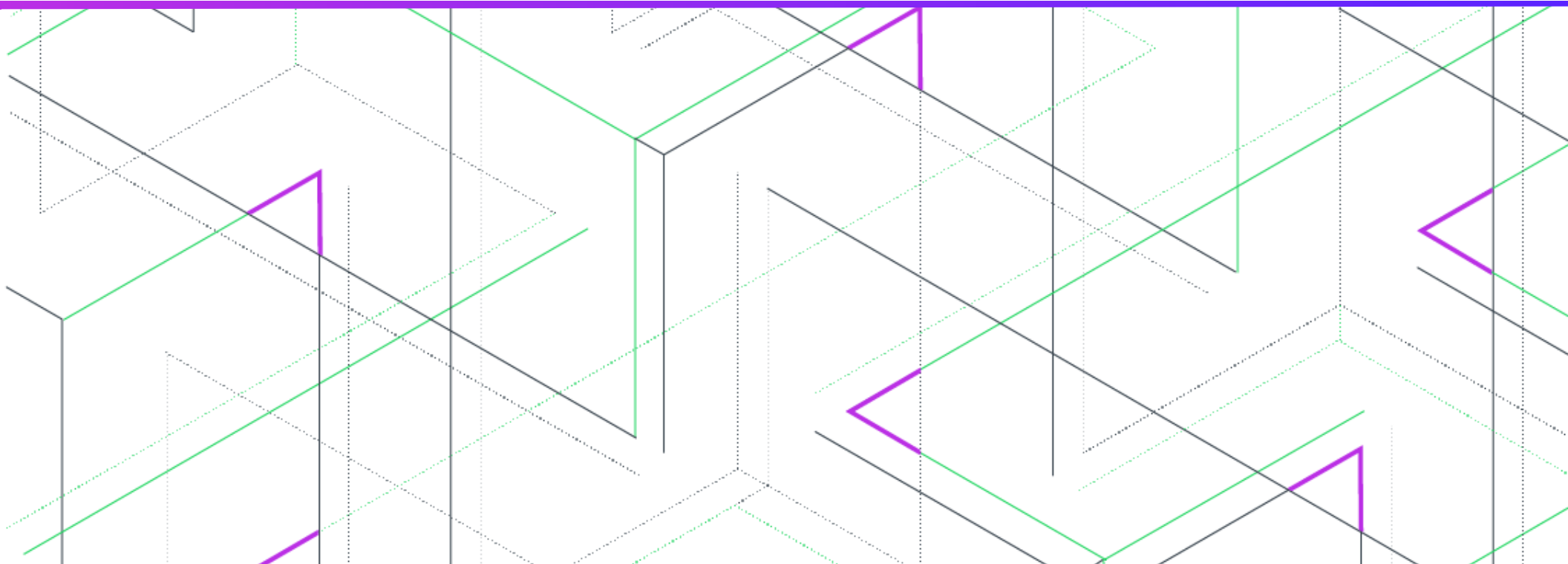
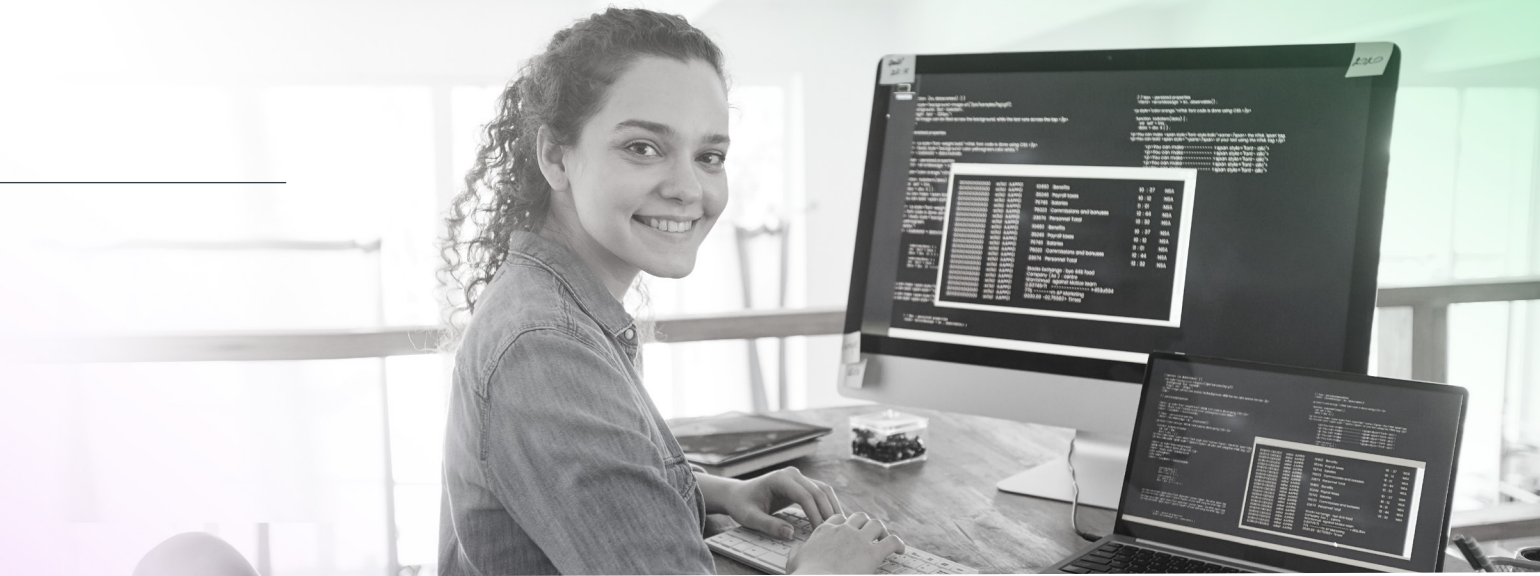


A Software Operations Guide to

Entitlement Management vs. Identity and Access Management





Introduction

When thinking about SaaS use rights, a good analogy is to consider how membership programs work at your local fitness center: You scan your card at the front desk and, depending on the package you've paid for, you're granted access to the facilities and classes your membership allows.

At the silver level, you'll get unlimited use of certain machines, but restrictions will be imposed on pool access, for example – incurring additional fees each time you swim. However, those on the platinum package can access all areas at no extra cost.

This is akin to how SaaS products generally work, with multiple subscription tiers and consumption models enabling different features, allowing users to select the most suitable package.

Furthermore, the fitness center can track usage and take proactive steps to re-engage you if you seem likely cancel, much in the same way SaaS producers monitor churn risk as part of **revenue optimization**.

Ultimately, in each case, the business wants to ensure customers only access the services they've paid for while maximizing the value given and received – looking for upsell opportunities where appropriate and targeting customer retention to grow Annual Recurring Revenue (ARR).

When it comes to setting SaaS use rights, suppliers often try to leverage existing investments in Identity and Access Management (IAM) systems, but soon realize the limitations and a need to combine IAM with purpose-built **Entitlement Management** technology. ■

What is IAM?

In simple terms, the IAM process validates the authenticity of users via an Identity Provider (IdP). Essentially, when logging into applications, users are prompted to provide proof of identity before gaining access, ensuring a level of security and compliance. Additionally, an IAM strategy allows you to assign roles within your organization, ensuring those working in different departments, for example, can access the products and services necessary for their job.

Identity and password information is securely stored within IAM systems, with changes efficiently handled and access blocked once users leave the organization. In short, IAM is very effective at managing group access to enterprise software.

However, there are serious drawbacks when SaaS producers apply this method to assigning use rights for application-specific roles.

What Is Identity and Access Management (IAM)?

USER AUTHENTICATION



Limitations of IAM for SaaS Use Rights

In conjunction with a Role-Based Access Control (RBAC) system, it's possible for publishers to use IAM to define separate roles and permissions within applications, but there are three major shortcomings:

1. **No feature tracking or usage insights**, which restricts the ability to monitor churn risk and assess upsell/cross-sell opportunities.
2. **Metered usage requires another system of record** – either third-party or homegrown – so usage-based billing relies on additional development and maintenance costs.
3. **Measuring overuse is complex**, with limited visibility for both the buyer and supplier, and enforcement often requires manual intervention.

Ultimately, IAM/RBAC frameworks are not designed with **software monetization** in mind, as pricing and packaging models need to be managed separately and integrated manually.

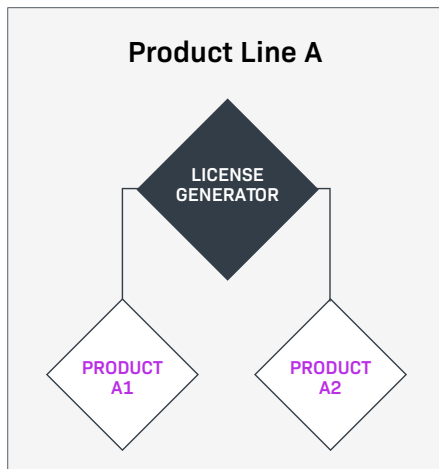
This somewhat basic approach to SaaS access management may work for some, but there is a more dynamic alternative.

Entitlement Management for SaaS

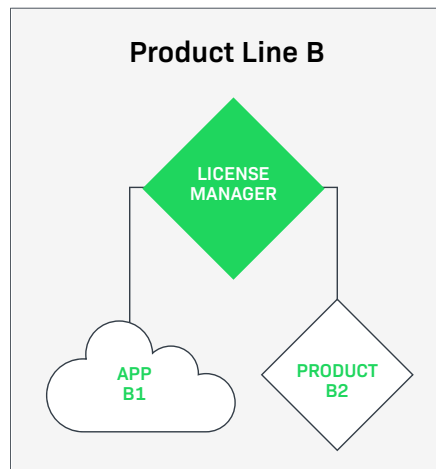
A centralized **entitlement management solution** is agnostic to **deployment models**, allowing you to offer advanced pricing and packaging for SaaS, on-premises, and hybrid environments.

For publishers with mature product portfolios spanning on-prem and SaaS, and perhaps with a history of acquired products through M&As, the complexity and cost of running siloed operations can be significant.

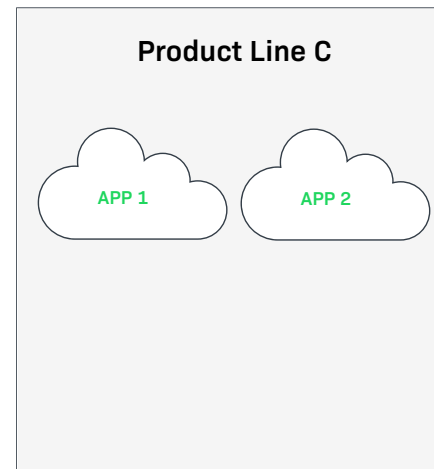
In the example below, the supplier has three product lines with separate enforcement solutions:



Product Line A: Legacy on-prem technology with homegrown licensing



Product Line B: Hybrid offerings using different back-office systems



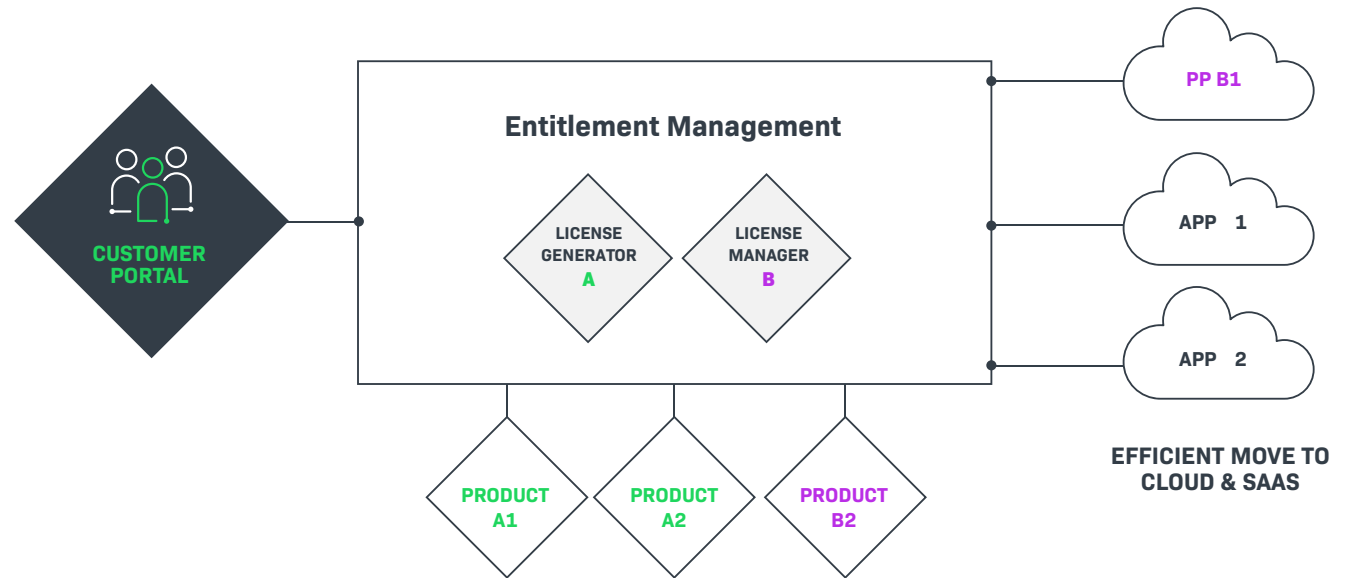
Product Line C: SaaS applications with independent processes



In this scenario, each product line has separate fulfillment and data collection engines, all adding to the operational overhead.



However, it is possible to consolidate the entitlement system into a single pane of glass, giving complete transparency into all products for reporting and billing – creating a unified experience for both customers and internal stakeholders, as outlined here:

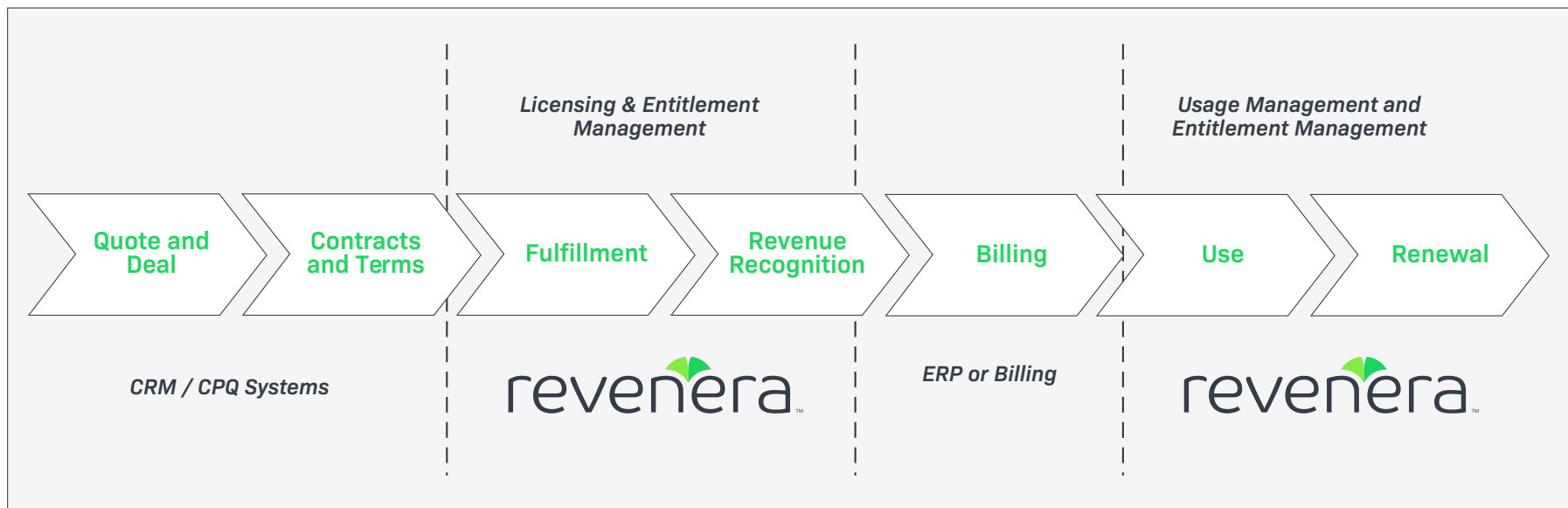


Essentially, entitlement management technology is purpose-built to manage use rights and data rather than stitching information together from disparate systems, enabling usage-based monetization with ease.

Measurement is inherent to entitlement management, facilitating a 'use rights enforcement system' that empowers both suppliers and customers to govern compliance.



Furthermore, consolidated entitlement management infrastructure allows you to streamline your **quote-to-cash (Q2C) process**, enabling automation and use rights monitoring from order to fulfillment, renewals, and billing, with the ability to analyze usage and act accordingly, as outlined in the chart below:



LEARN MORE

Mastering Entitlement Management and Improving Operational Efficiency

You can learn more about consolidating Q2C as part of modern entitlement management in this free webinar with IDC's Research Director, Mark Thomason

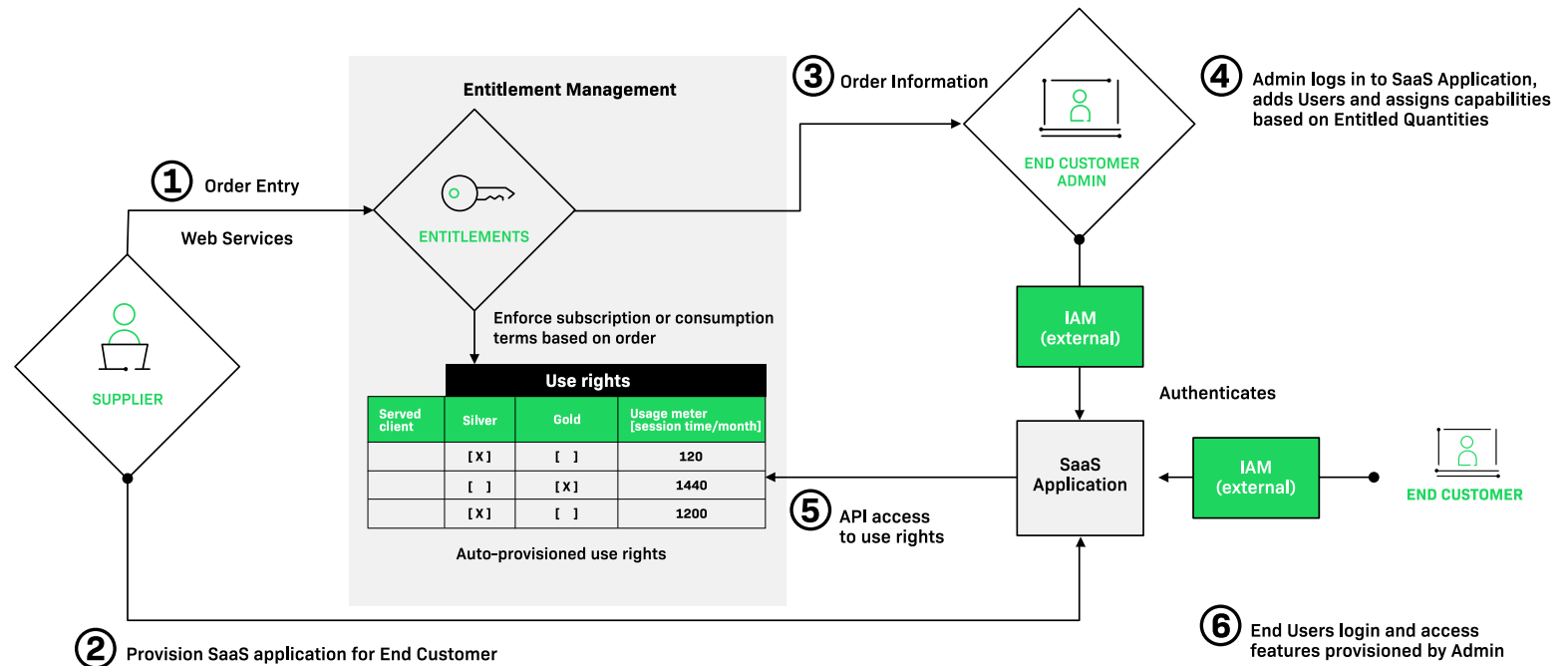


[WATCH THE WEBINAR >](#)

SaaS Entitlement Scenario



In this diagram, you can see how SaaS entitlement management works:



In this scenario, once an order is placed, use rights are auto-provisioned, i.e., immediately made available to the customer. Typically, an email is sent to a key contact at the customer, detailing how to log in and assign their users different capabilities within the application. The mapping of use rights is maintained and enforced within the entitlement system rather than the application – keeping track of assignments, when specific features have been used, reporting of metered components, etc.

IAM still plays a role in this process, authenticating users at the customer's end, but, again, the mapping and tracking of use rights is maintained within the entitlement system.

Key Benefits of SaaS Entitlement Management

In terms of stimulating revenue growth, a centralized entitlement management solution can help you:

- Accelerate time-to-market for new products and features, with auto-provisioned use rights
- Increase renewal rates with actionable insights into usage
- Recover lost revenue by tracking overuse (both intentional and unintentional)
- Improve customer experience with consistent delivery across all product lines
- Boost channel sales and support with visibility into reporting, billing, and renewal data

Additionally, centralized entitlement management enables multiple operational efficiencies, including:

- Reduced need to build and maintain homegrown systems
- Future-proof technology that can easily adapt to new monetization models
- Streamlined processes to scale with your business
- Self-service for customers and channel partners
- Fewer support tickets due to standardizing on a single platform

In our experience, these streamlined operations can reduce your cost by up to 10% while freeing up resources for more strategic projects, so the ongoing ROI of an integrated entitlement management system is tangible.



YOU MAY BE INTERESTED...

Software Entitlement Management Guide

[READ THE BLOG >](#)

Forward Planning

As **61% of technology companies plan to increase SaaS delivery by 2026**, it's vital to consider what use rights management system is best suited to your future monetization strategy.

If you're in the process of a **SaaS transition**, it can be tempting to fall back on the IAM approach that may have served you well for on-premises products. However, many find the necessary development and maintenance drains resources from core competencies that could be focused on delivering customer value.



The upfront cost of centralization may be higher than IAM, but there are many long-term benefits of entitlement management for SaaS use rights.

IAM

- Authenticate Users
- Assign Organization Roles
- Enforce Access Rights integrated with RBAC



Entitlement Management

- Monetize software
- Grant, resolve, enforce, revoke and administer fine-grained access entitlements
- Provide single pane of glass
- Integrate into Q2C

Additionally, IAM alone doesn't allow usage data collection, which is **crucial to monetization initiatives**, and the operational overhead is multiplied when relying on disparate back-end systems.

Entitlement management in conjunction with IAM, on the other hand, is a flexible solution that allows you to manage access rights and measure usage across multiple product lines, reconciling data into a single source of truth.

NEXT STEPS

If you need guidance on how to manage SaaS usage, our expert entitlement management team is here to help. Please contact us today and we can arrange a time to talk that suits you.

LEARN MORE >

APPLICABLE CASE STUDIES



infor  **thingworx®**

Our *Infor* and *ThingWorx* case studies provide an insight into how Revenera solutions can help you introduce SaaS monetization models and improve customer experiences.

YOU MAY BE INTERESTED...



A Software Operations Guide to Entitlement Management vs. Billing Management and Subscription Management

READ THE EBOOK >



Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud.
www.revenera.com