WHITEPAPER

The Advantages of a Physical Identity & Access Management (PIAM) Platform as Software as a Service

High security. Fast deployment.
Always up to date.

Table of Contents

Introduction

Organisations across every sector face a common challenge: managing physical identities — employees, contractors, visitors — alongside their access to buildings, secure areas, and sensitive facilities. Traditionally, this has required significant capital investment in on-premises software and dedicated infrastructure teams to operate and maintain it.

Software as a Service (SaaS) fundamentally changes this equation. By moving infrastructure ownership to a specialist provider, organisations gain enterprise-grade capability without enterprise-scale IT overhead. When this delivery model is applied to Physical Identity & Access Management (PIAM), the benefits are even more pronounced: faster deployment, lower total cost of ownership, stronger support for regulatory obligations, and built-in scalability.

This Whitepaper presents the strategic case for SaaS as the delivery model for PIAM, and introduces how ID-ware's PIAM Suite enables organisations of all sizes to benefit from a high-end enterprise-class platform, without the traditional investment burden. Where SaaS is not permitted, the platform is also available as private cloud, managed hosting or on-premises.

1. What is Physical Identity & Access Management?

Physical Identity & Access Management (PIAM) is a discipline that unifies the management of people's identities with the control of their physical access to facilities, buildings, and restricted areas. A PIAM platform acts as the single source of truth for who is authorised to be where — and under what conditions.

Credential Management

Full lifecycle of physical access credentials — from design and personalisation to issuance and revocation.

Access Management

Workflow-driven control of physical access permissions across an organisation's entire site portfolio.

Visitor Management

Automated visitor registration, pre-registration, identity verification, and check-in/check-out workflows.

Contractor Management

Managed onboarding and access control for third-party workers with document compliance and auto-revocation.

User Self-Service & Photon

User Self-Service Portal empowering employees to manage card data, access requests, and passport-style photos.

Integrations

Connectors to HR and directory systems, access control and other third-party systems like parking, locker or payment management.

Without a unified PIAM platform, organisations typically operate a patchwork of siloed tools — creating compliance gaps, administrative overhead, and unnecessary security risk.

2. The Case for SaaS in Enterprise Software

Key advantage

Enterprise-grade PIAM — without enterprise-scale IT overhead.

SaaS software is hosted by a provider in the cloud and accessed via subscription — not purchased, installed, or maintained on-premises. Over the past decade it has become the dominant model for enterprise software adoption.

2.1 WHY SAAS CHANGES THE EQUATION

Moving from on-premises to managed SaaS fundamentally changes the cost structure, risk profile and operational burden for any organisation. Responsibility for infrastructure, availability and platform security passes to a provider whose core business is running that platform, while the organisation keeps full control over its processes, roles and data. The comparison below sets out what changes on each side.

ON-PREMISES

- High upfront investment
- Internal IT team required
- Your risk & compliance burden
- Delayed upgrades
- Capacity planning risk
- You own disaster recovery
- Compliance on your team

Complexity grows vs. Simplicity scales

MANAGED SAAS

- Predictable subscription
- Platform team included
- Risk transferred to provider
- Always up to date
- Built-in redundancy
- Elastic, on-demand scaling
- Supports your compliance

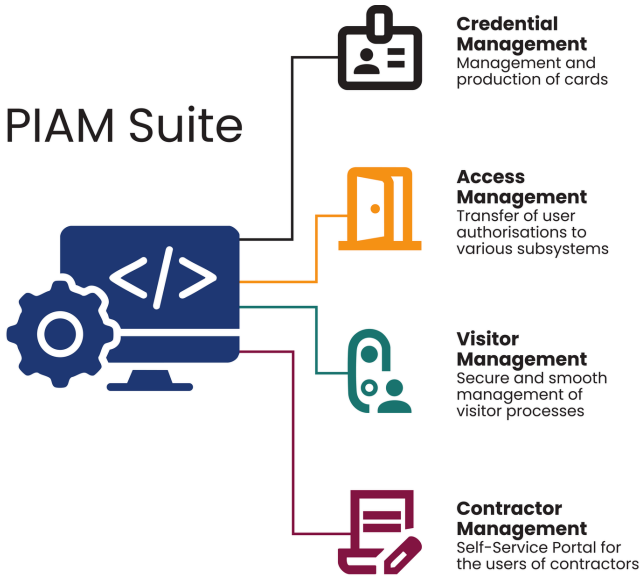
KEY INSIGHT

Organisations that deploy a PIAM platform as SaaS not only reduce operational cost — they also close a significant security and evidence gap that traditional on-premises deployments leave open.

3. ID-ware's PIAM SaaS Offering

ID-ware is a specialist provider of Physical Identity & Access Management (PIAM) solutions with over 20 years of experience serving organisations across Europe and beyond. The ID-ware PIAM Suite as SaaS helps organisations to streamline their physical identity and access management — reducing cost, complexity, and compliance risk in a single step.

3.1 THE ID-WARE PIAM SUITE



3.2 THE ADVANTAGES OF THE ID-WARE PIAM SUITE AS SAAS

Delivering the PIAM Suite as a SaaS solution gives organisations enterprise-grade physical identity and access management — without the infrastructure burden. ID-ware takes full responsibility for hosting, uptime, updates, and the security of the platform.

High Security
European hosting — data never leaves certified EU data centres

Fast Deployment
Same-day activation and environment availability in the public SaaS model

High Availability
99.9% uptime, built-in redundancy & automated failover

Customisation
Highly configurable functional scope to match your processes

Continuous Updates
All patches & releases automatically managed by ID-ware

Compliance support
Supports you to comply with your NIS2, DORA, GDPR & ISO 27001 obligations

4. The Platform Engineering Team (PET)

Your infrastructure.
Our responsibility.

ID-ware's SaaS delivery is underpinned by a dedicated Platform Engineering Team (PET) — experienced Platform Engineers, Cloud Architects, and Cloud Engineers who design, build, and operate the underlying cloud infrastructure so your teams never have to.

The PET's mandate spans five core domains

Each domain is fully managed by ID-ware — from infrastructure provisioning to compliance monitoring — so your organisation can focus entirely on using the PIAM Suite to drive business value.

WHAT THIS MEANS FOR YOU

Always current

Every update and security patch is deployed automatically by ID-ware — your environment always runs the latest version, with no effort required from your team.

Built to scale

Infrastructure scales automatically with your organisation's needs — no capacity planning, no over-provisioning risk, no performance bottlenecks.

Engineered for resilience

Self-healing architecture and automated failover keep your PIAM platform running at all times — backed by continuous monitoring from the ID-ware team.

Zero infrastructure overhead — your teams stay focused entirely on using the PIAM Suite — not maintaining servers, managing patches or planning for capacity.

4.1 THE PLATFORM ENGINEERING TEAM (PET) — FIVE CORE DOMAINS

The PET's five core domains work together as an integrated whole — each essential to delivering a platform that is secure, available, compliant and always current. Every domain is fully managed by ID-ware, so your organisation can focus entirely on using the PIAM Suite to drive business value.

5. Common Concerns — and how we answer them

Organisations considering a move to managed SaaS often raise the same set of questions. Here are the answers.

As the following responses show, **common objections against SaaS do not hold up under scrutiny** — and in most cases, the managed model addresses each concern more effectively than a self-hosted alternative ever could.

Will a SaaS platform accommodate our unique processes?

The ID-ware PIAM Suite is **highly configurable**. The modular architecture means organisations adopt **only the capabilities they need** and configure them to match their processes — not the other way around.

We are concerned about data security in the cloud.

All data is hosted in **European-certified data centres**, supporting GDPR data residency requirements. The platform includes **centralised security management including infrastructure security**. ID-ware is **ISO 9001 and ISO 27001 certified** and participates in TISAX.

We are worried about being locked into a subscription.

ID-ware offers **flexible contract terms** designed to grow with your organisation. Scalability is built into both the solution and the commercial model — **expand or adjust your scope** as requirements evolve, without rigid multi-year commitments.

What happens when we need to scale or requirements change?

The ID-ware PIAM Suite **scales elastically** with your organisation. Adding sites, users, or modules requires **no infrastructure changes** on your side — ID-ware's PET handles provisioning, capacity, and rollout. You pay for what you use.

Is SaaS really suitable for large, professional organisations?

SaaS is the **dominant software model for enterprises worldwide**. The majority of Fortune 500 companies run critical processes on SaaS. The ID-ware PIAM Suite as SaaS can be used by organisations of any size, but is **purpose-built for complex deployments**.

We already have an on-premises system — is migration complex?

ID-ware's **structured onboarding** ensures a smooth transition from any existing system. Environments in the **public SaaS model are available same day**, and ID-ware specialists guide the migration from data mapping to go-live — **minimising disruption** throughout.

6. Total Cost of Ownership (TCO): On-premises vs. SaaS

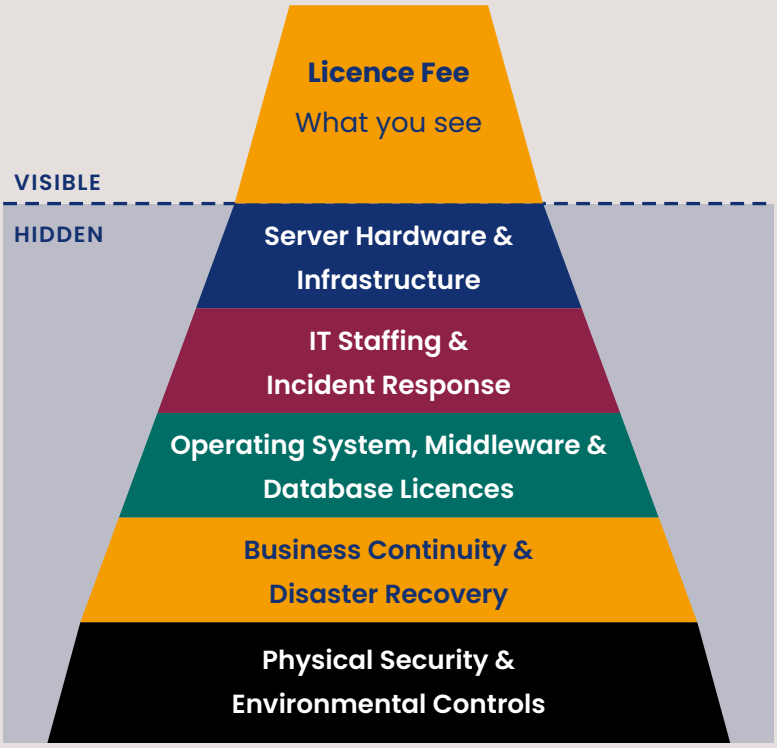
A structured Total Cost of Ownership (TCO) analysis reveals the true financial and operational picture when comparing self-hosting against SaaS. Across every dimension — infrastructure, staffing, compliance, and scalability — the SaaS model consistently delivers lower risk, lower cost, and greater operational simplicity.

6.1 THE HIDDEN COSTS OF ON-PREMISES DEPLOYMENT

The licence fee is only the tip of the iceberg

On-premises Total Cost of Ownership consistently exceeds initial estimates. The costs below the surface are where organisations get caught out.

3–5×
true Total Cost of Ownership vs. licence cost



BEYOND DIRECT COST

Several factors never appear on an invoice, yet they determine what a deployment really costs over its lifetime.

Speed of innovation

Self-operated installations require every update to be tested and rolled out internally. In SaaS, new capabilities are available as soon as they are released.

Service levels

A self-operated platform needs internally defined and internally resourced service levels. SaaS is delivered against an agreed SLA.

Financial planning

On-premises combines capital investment with fluctuating operating costs. SaaS is a single, predictable operating expense.

Business continuity

A self-operated deployment needs its own disaster recovery concept. Failover across availability zones is part of the SaaS platform.

6.2 ON-PREMISES VS. SAAS COMPARED

Dimension	On-premises	ID-ware SaaS
Infrastructure	Investment in hardware and/or data centre capacity required.	Infrastructure is included in the SaaS price. No separate investment needed.
Operations & staffing	Dedicated internal IT team required for monitoring, backup, patching, and high availability.	ID-ware handles all operations, updates, monitoring, and security.
Security & compliance	Organisation is solely responsible for GDPR, certifications, and penetration testing.	ID-ware holds relevant ISO 27001 and ISO 9001 certifications, centralised security, and audit trails as standard.
Scalability	Additional capacity requires investment. Risk of over- or under-provisioning.	On-demand scaling. Costs grow linearly with usage and over-provisioning risk is eliminated.
Overall assessment	Appropriate where data sovereignty rules, internal cloud policy, or substantial existing IT infrastructure require it — a model ID-ware fully supports.	More economical, lower risk, lower fixed costs, and better scalability for the majority of organisations.

99.9%
platform availability — built into every ID-ware SaaS deployment

Day 1
environment availability on sign-up in the public SaaS model

TCO Summary — The responsible choice for PIAM

SaaS hosting eliminates capital expenditure, transfers operational risk to ID-ware, guarantees contractual SLAs, and delivers continuous access to the latest capabilities — within a predictable subscription cost.

For PIAM, where compliance, security and availability are non-negotiable, this model is not merely convenient — it is the responsible choice.

6.3 COMPANY PROFILES AND TOTAL COST OF OWNERSHIP

SaaS or on-premises? Organisation size does not decide this question. What decides it is **the shape of the investment** and the way an organisation wants to carry operational and security responsibility.

On-premises means a substantial upfront outlay for hardware, licences and set-up, followed by internal staff to carry the running costs and by renewal investments whenever hardware or versions reach end of life. The commitment is made years before the benefit is fully realised.

SaaS converts that into a defined recurring amount, with no team required for maintenance, patching or updates, and no capital tied up in infrastructure.

Security belongs in the same calculation. A managed SaaS environment is in most cases **more secure than a self-operated installation**. Rather than waiting for an internal maintenance window, patches and security updates take effect immediately, and the platform is monitored centrally. The three company profiles below show how this affects the total cost of ownership at different scales.

COMPANY PROFILE A

Smaller and medium-sized organisations

- No platform team is needed: operations, patching and backups are handled by ID-ware
- The dependency on one or two internal specialists disappears
- Enterprise-grade availability without enterprise-scale IT
- A plannable recurring cost instead of an upfront investment for an on-premises installation

Verdict: SaaS is the clear choice.

COMPANY PROFILE B

Larger organisations with established IT operations

- Specialists stay on business projects instead of platform maintenance
- Service levels are contractual rather than internally resourced
- Operational risk sits with ID-ware, not with your team
- Extra users and sites are absorbed without a new investment cycle

Verdict: SaaS is strong on opportunity cost and risk transfer.

COMPANY PROFILE C

Multi-site organisations and group structures

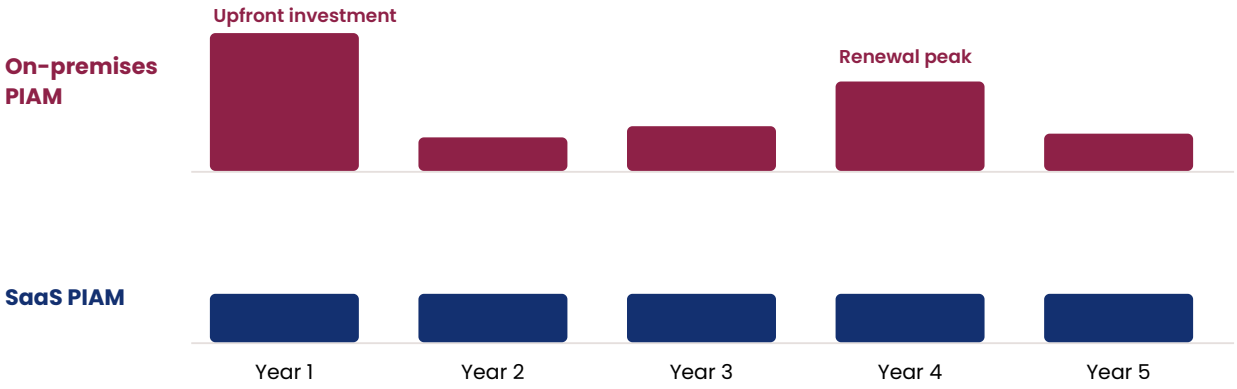
- No local IT presence needed at individual sites
- A uniform security level and consistent reporting, supporting audit readiness at all sites
- A new site or acquisition is a configuration step, not a new project
- Capacity for new sites and users is provisioned by ID-ware, without procurement or lead time

Verdict: SaaS scales smoothly wherever the group grows.

The comparison remains a structural one: it describes how cost and effort are distributed, not what a specific configuration costs. On that basis, the points below turn the three company profiles into a practical check. In most organisations several of them apply at once, and it is that combination which makes the case decisive.

THE SHAPE OF THE INVESTMENT

On-premises concentrates spend in a large initial investment and later renewal peaks. SaaS spreads the same capability across a predictable recurring amount.



Illustrative representation of how spend is distributed over time. Not absolute figures.

HOW SAAS PAYS OFF

- The investment is a **defined recurring amount** rather than a large upfront outlay.
- New releases **reach production quickly**, without an internal rollout project each time.
- **No dedicated platform operations team** is needed any more.
- Availability and recovery are **guaranteed contractually** rather than resourced internally.
- **No internal capacity has to be built up** for maintenance, patching and updates.

NOTE: IF SAAS IS NOT AN OPTION FOR YOU

In some environments, for example in the public sector, in critical infrastructure or in other high-risk settings, internal policy or sector regulation may require a different deployment model. ID-ware also offers **private cloud, managed cloud hosting and on-premises deployment**, each with the same functional software scope and the same support organisation.

Organisations that currently run an on-premises installation can move to a SaaS model at any time. The transition is planned thoroughly and in close collaboration with your teams, and is supported throughout by ID-ware.

7. Typical ID-ware SaaS deployments by sector

The ID-ware PIAM Suite as SaaS is deployed across sectors that manage physical access at scale. The examples below are typical rather than exhaustive: each sector brings distinct requirements, and each is addressed by the same platform.

Education & University

Managing large, diverse populations of students, staff, and visitors across multiple campuses with efficient mass enrolment.

Industry & Manufacturing

Controlling access to production areas and hazardous zones, including visitor and contractor management, supporting ISO, GDPR and NIS2 requirements.

Public Sector & Critical Infrastructure

Supporting stringent security and data sovereignty requirements with a European-hosted solution as a single-tenant private cloud (if that is no option, the ID-ware PIAM Suite can be deployed on-premises).

Aerospace & Defence

Managing strictly tiered access to restricted areas, integrating with personnel vetting processes and delivering the auditability required for security clearance obligations.

Financial Services

Supporting DORA resilience requirements and sector audit obligations for physical access.

Healthcare & Medical

Managing access to patient areas, pharmaceutical stores, and research facilities with full audit trails.

8. Conclusion

Physical Identity & Access Management (PIAM) is a critical discipline that sits at the heart of physical security, operational efficiency, and regulatory compliance. Yet many organisations still operate legacy, on-premises PIAM tooling that is under-resourced and increasingly misaligned with their risk and compliance obligations.

The SaaS delivery model resolves this tension. By transferring infrastructure ownership to a specialist provider, organisations access enterprise-grade capability with predictable cost, strong support for their compliance requirements, and zero infrastructure burden.

ID-ware's PIAM Suite as SaaS represents the logical evolution of physical access management. With European hosting and a dedicated Platform Engineering Team, ID-ware provides a foundation organisations can build upon.

Netherlands: +31 70 337 1500 Germany: +49 69 210 8555 60 UK: +44 20 8050 2648 info@id-ware.com