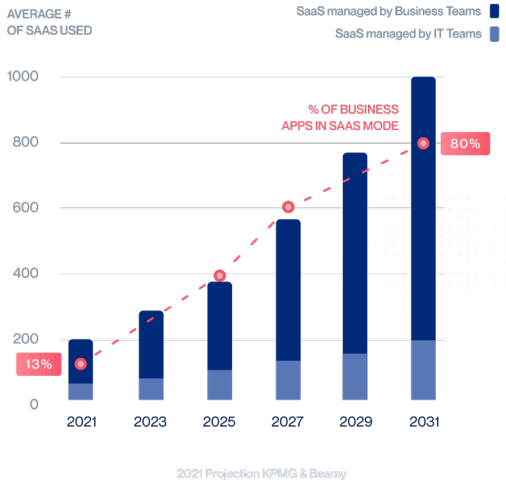
Managing the SaaS Revolution: the priority for large organisations of 2023-2027

The introduction of Software-as-a-Service (SaaS) in the late 90s marked the beginning of a paradigm shift. Since then, SaaS applications have proliferated exponentially, and in the process, Shadow IT has thrived unnoticed by IT teams, who often looked the other way.

The inevitable rise of Shadow IT: the urgent need to act for large organisations

Software-as-a-Service (SaaS) has profoundly changed the IT ecosystem. It is reshaping the way large organisations digitalise, reflecting societal changes driven by the new tech-savvy generations, rapid technological advances and trends towards remote working.



The adoption of SaaS by employees shows no signs of slowing down. It is 'inevitable'.

As of 2023, global SaaS spending is projected to hit $197 billion, an 18% increase from 2022 (Gartner). KPMG predicts that companies will quintuple their SaaS apps and increase budgets ninefold in the next decade.

By 2031, 80% of business apps will be SaaS-based, up from 13% in 2021.

By 2027, 75% of employees will acquire, modify and create technology outside IT's visibility. *(Gartner 2023)*

The reason for the SaaS popularity (and the spread of Shadow IT) lies in its decentralised nature. Employees leverage user-friendly and often free applications to independently address their daily challenges. It enables them to do their jobs better, stimulating innovation, productivity and efficiency. However, they often bypass IT departments when choosing applications. Statistics reveal that by 2027, 75% of employees will acquire, modify and create technology outside IT's visibility (Gartner, 2023).

> **Shadow IT is inevitable. [...] CIOs that don't see much shadow IT in their organizations are not looking for it or are looking in the wrong place.**
> (Gartner, 2017)

While SaaS growth and IT democratisation hold immense potential, the lack of governance has led to uncontrolled challenges because of Shadow IT. By failing to promptly grasp the extent of their SaaS sprawl, companies lose valuable time in proactively addressing the forthcoming surge in SaaS usage. It has become urgent for organisations to assess the risk associated with their use and implement appropriate security measures.

Shadow IT: the multi-faceted risks

IT departments are often only aware of a third of the SaaS applications in use (Gartner Market Guide, 2022), which raises considerable risks and challenges within their organisation. Gartner has revealed that by 2027, those that fail to achieve centralised visibility and manage SaaS life cycles will overspend on SaaS by at least 25% and be 5 times more exposed to cyber risks or data loss.

The risks associated with the use of SaaS applications can take various forms: security, compliance concerns, financial implications, or operational and efficiency challenges.

Security Risks

Shadow IT poses severe security threats as these unapproved applications operate beyond organisational security measures, making them targets for cyberattacks and data breaches. Randori's State of Attack Surface Management 2022 report reveals that nearly 70% of organisations have been compromised by shadow IT in the past year because of a lack of visibility over their IT assets by the IT department. Additionally, IBM's 2022 findings show that 45% of companies suffered cloud-based data breaches, costing an average of $4.35 million.

Compliance Concerns

Shadow IT exposes organisations to compliance risks since these applications often evade scrutiny. Regulations like GDPR and industry standards like HIPAA and DORA necessitate meticulous compliance, especially for large enterprises subject to rigorous oversight. In a recent example, in August 2023, the Commodity

Futures Trading Commission issued orders for four financial institutions to pay $260 million for the use of non-approved methods of communication (WhatsApp, Signal…) to engage in business-related communications, in violation of firm policy.

Financial Implications

Apart from compliance fines and data breach costs, unknown applications can lead to overspending on unused IT resources. According to Gartner, companies will overspend $750 million on unused features of IT software this year alone. This complicates IT budget management, particularly in larger enterprises where 30-40% of the IT budget goes to unknown applications. The result is an underestimation of the technical budget, which hampers the overall negotiation of enterprise-wide contracts, particularly because of certain abusive conditions imposed by SaaS providers (price increases, unclear renewal conditions, etc.).

Lack of operational efficiency

Shadow IT can have an impact on the IS and bring unexpected challenges for IT teams, due to its total lack of planning and good IT practice. This forces the technical team to provide unanticipated support including setting up workflow configurations, identifying risks, managing data, and so on. All tasks that could have been avoided with prior consultation.

This results in diverting end-users and IT teams from their core tasks as well as frustration and tensions between teams: BUs blame IT for not providing the necessary tools and visibility, while IT points fingers at the business for not adhering to established guidelines and protocols.

It becomes crucial for IT departments to address those risks and educate BUs more effectively, as they operate in an increasingly complex and regulated environment, particularly in the European market, due to stricter regulations.

SHADOW IT

Shadow IT is already pervasive

80%

of employees admit using IT solutions without the approval of IT

Frost & Sullivan, 2020

SAAS GROWTH

SaaS growth is accelerating

x5

of projected SaaS growth over 2021-2031

Projection KPMG, 2021

COMPLIANCE

Regulatory compliance is strengthening

€1.5bn

GDPR fines issued in the first half of 2023

Atlas VPN, 2023

SECURITY

Cybersecurity threat is rising

48%

cyberattacks in 2022 versus 2021

Check Point: Cloud Security Report - 2022

FINANCIAL

Losing control over their IT budget

30-40%

IT spending goes to shadow IT in large enterprises

Gartner, 2017

From Shadow IT to Shadow AI: a new risk dimension

The rise of generative AI (GenAI) has led to the emergence of Shadow AI, adding a new layer of risk to those of Shadow IT. Employees are increasingly using these tools without proper training or guidance. A Fishbowl study found that 68% of employees are using AI tools like ChatGPT without notifying superiors or IT departments. This unchecked adoption introduces major legal and security risks, which may exceed those of Shadow IT.

- **Confidential Data Risks:** Unauthorised use of AI tools can result in data breaches, as employees may inadvertent input sensitive information (personal or business-sensitive data). This data is fed into AI models and unintentionally shared, exposing confidential information to the public. The Samsung example strikingly highlights the need to train employees in these tools. Samsung engineers introduced some of the company's confidential code into ChatGPT in the hope of correcting problems, instead causing a security breach. In response, the company quickly banned all staff from accessing the AI tools.

- **Compliance Risks**: The disclosure of personal information on this type of tool also violates current regulations such as the GDPR. When employees input sensitive data into unauthorised AI tools, they not only expose the company's liability leading to potential penalties and but also put its reputation at risk.

- **Bugs and Vulnerabilities**: A number of recent incidents have highlighted vulnerabilities. For example, a bug in an open-source library used by ChatGPT allowing access to others' conversation history and exposing sensitive internal discussions or confidential client information from companies. Similarly, Microsoft's AI research team accidentally exposed 38 terabytes of private data (passwords and more than 30K internal Microsoft Teams messages).

Like SaaS, AI is now integral part of employee work habits. Obstructing its use would be counter-productive. IT leaders must prioritise managing the hundreds of tools that keep crawling into their IS. Yet striking a balance between solid governance and business needs for autonomy is proving to be a daunting challenge, especially when using a variety of sources/tools to make sense of this ecosystem.

Instead, IT teams need to establish a framework that maximises the full potential of this technology, while ensuring compliance with the company's policy on confidentiality and compliance, in order to minimise the risks.

From Shadow IT to Business-Led IT

Expecting the IT department to oversee every technological initiative and address every business need is impractical and impedes an organisation's progress. Eradicating Shadow IT is not a viable solution.

This is where the distinction between Business-Led IT and Shadow IT becomes apparent. Business-Led IT adds value and is usually implemented with a clear commitment. The democratisation of IT within a company represents a transformation process that has an impact on all facets of business and IT operations. It offers significant opportunities for growth and empowerment for both employees and IT teams, subject to effective management and security measures.

The need for a governance framework

IT teams typically establish robust frameworks to address associated risks and exert high-level governance. It also requires redefining the relationships with the different stakeholders in the business and diversifying the IT's role in managing IT by recognising the realities and benefits of business-led IT projects.

To move to a business and value-led approach to IT, CIOs need to address four problems:

- **Transparency**: Achieving transparency and coherence across business by consolidating, categorising, and communicating a "single source of truth" on technology investments.
- **Risk**: Mitigating risk by offering services to support requirements and adopting a flexible governance approach to determine when intervention is necessary and when it isn't.
- **Empowerment**: Minimising digital friction by making tools, platforms, standards, and principles to clarify and enhance decision-making.
- **Accountability**: Clarifying that if a business unit deploys a solution, it also assumes ownership and responsibility for it.

Discover our latest white paper & read Decathlon's exclusive testimonial on implementing an effective SaaS governance.

The role of SMPs: between autonomy and risk management

A SaaS Management Platform (SMP) plays a central role in addressing these 4 challenges and helping CIOs shift to a modern approach to

managing their SaaS landscape. The SMP acts as a centralised hub with a comprehensive set of functionalities, providing all stakeholders with clear visibility. This facilitates risk management and promotes greater autonomy and collaboration between teams.

> **Managing multi-SaaS environments with disparate consoles results in sprawl, lack of control and overspending. SaaS management platforms simplify this process. [...] SMPs offer a complete set of capabilities, whereas adjacent market tools (SAM, CASB, SSE...) provide only some of the capabilities.**
> (*Gartner Market Guide 2022)*

The benefits offered by SMPs extend to an enhanced ability to monitor and govern SaaS applications while guiding Business Units. They provide a holistic solution to the proliferation of SaaS applications, enabling organisations to efficiently discover, manage, automate, optimise, govern, protect, and enable them.

Moreover, SMPs can also establish an 'App Center' to minimise the use of unauthorised SaaS, while sharing approved applications across all relevant stakeholders. Automation reduces the burden on IT teams while fostering collaboration between teams across various stages of the SaaS lifecycle. Restoring collaboration paves the way for greater innovation and performance.

Learn here about SMP capabilities and why it remains on Gartner's Hype Cycles and Market Guide.

As the SaaS landscape continues to grow significantly and impact more and more business operations, trying to fight Shadow IT will prove counterproductive.

Instead, CIOs need to provide appropriate advice and support to enable business-led IT. CIOs will increasingly play a leading role in shaping the organisation's roadmap. To do this, they must act as facilitators and trusted business partners, ensuring that the organisation adapts its operational framework effectively.

This represents a significant opportunity for CIOs to harness value from IT by actively guiding and supporting business units in the process of reducing risk and optimising their digital initiatives.

To accomplish this transformation efficiently, the adoption of SMP will become imperative. It will support CIOs and IT managers in maximising

About Beamy

Beamy is the leader in SaaS (Software-as-a-Service) Management for large organisations, and its customers include key accounts across a wide range of sectors: LVMH, BNP Paribas, Decathlon, Kingfisher and many others.

Large companies are facing a surge in the number of SaaS applications, often deployed by business departments (HR, Marketing, Product) without informing IT teams. This underground digitisation (or Shadow IT) is pervasive and generates major security and compliance risks.

Beamy helps CIOs and IT departments to optimise their SaaS ecosystem using a unique platform tailored to the complex and regulated environment of large companies. It has the ability to automatically and continuously detect and index all SaaS used within the organisation, including those in Shadow IT. As a result, IT managers can manage and monitor all applications effectively, reducing risk while meeting employees' needs. At the same time, business users can select their preferred SaaS applications within a defined governance framework.

Beamy

Beamy - 6, rue Auber - 75009 Paris.

beamy.io

October 2023