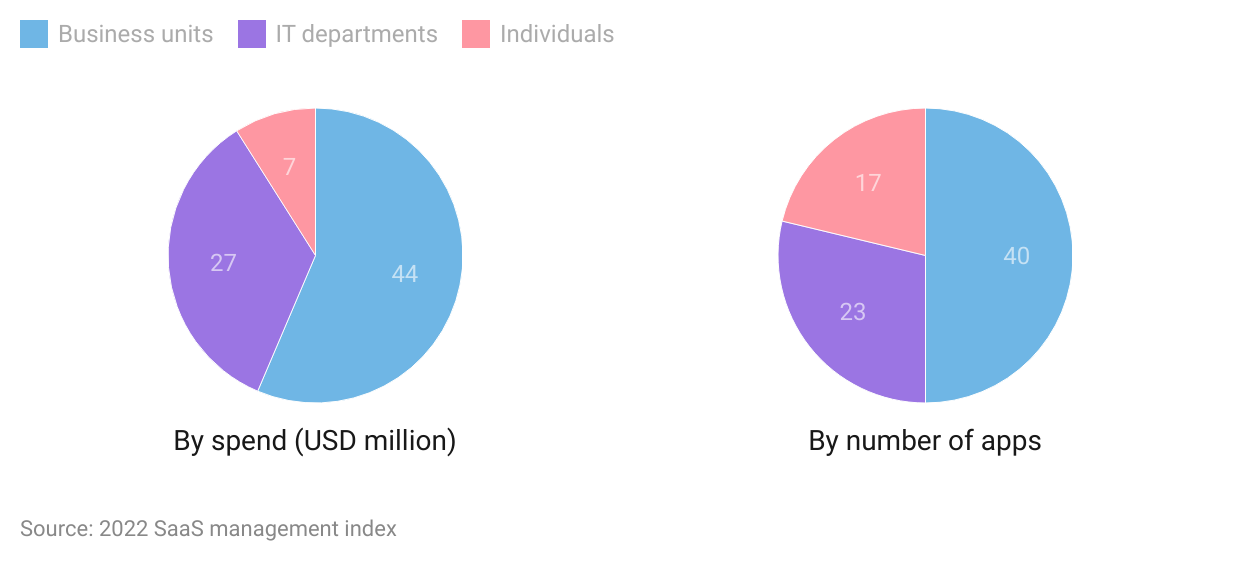
# **B2B SaaS Management Platforms: Overview**

****

### **Decentralized decision-making at firms, leading to a rise in Shadow IT**

Gone are the days when the IT department held sway over what software and applications were accepted to be used at a firm. Many firms adopt a decentralized business model, where individual business units now have greater discretion and flexibility over the software and applications they use. As a result, [studies done in 2022](https://zylo.com/reports/saas-management-index-2022/) showed that only 27% of an organization's SaaS applications were directly managed by IT.

### **IT departments have a declining role in a firm's SaaS ownership.**



This gives rise to [shadow IT](https://www.forcepoint.com/cyber-edu/shadow-it), the use of IT systems, software, applications, and other services without the IT department's explicit approval. While shadow IT provides many benefits to firms in terms of helping to drive innovation and improve employer productivity through the greater flexibility it provides, it also gives rise to a higher incidence of data breaches and compliance-related risks. [Studies have shown](https://www.gartner.com/smarterwithgartner/is-the-cloud-secure) that 99% of cloud breaches are caused by applications or user configuration errors, usually due to the lack of intervention from IT department specialists. In addition, this has resulted in non-trivial cost increases across organizations due to the lack of visibility of a firm's SaaS stack, leading to a duplication of apps, surprise renewals, un-revoked licenses, and wastage of available application licenses.

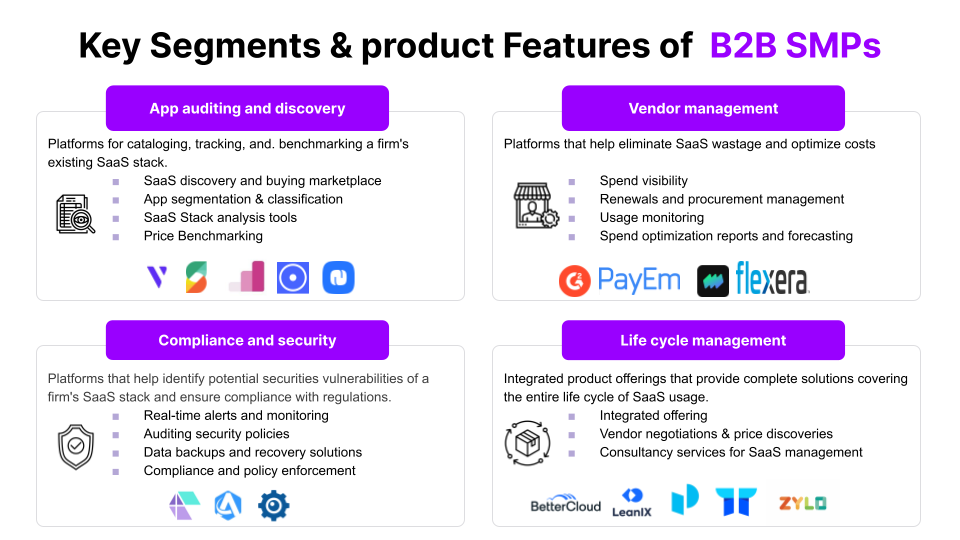
Hence, firms have a need for tools to provide visibility on a firm's shadow IT to help identify and reduce security and compliance vulnerabilities as well as monitor usage and renewal cycles for better cost management.

### 

**What are B2B SMPs?**

SMPs are B2B cloud-based platforms designed for IT and other administrators of business units for managing the day-to-day activities of SaaS applications used by a firm. A key objective of SMPs is to provide information and tools for business leaders to manage their portfolios of SaaS applications effectively.

### 



### Source: Created by SPEEDA Edge

However, we exclude the following areas when selecting companies for this industry:

1. Subscription-management platforms that are primarily for the B2C market
2. Financial operations platforms for managing a firm's revenue life cycle, which include payables, receivables, and billing management. E.g., Maxio, Changebee
3. Platforms for managing and optimizing a firm's cloud infrastructure (covered under [Cloud Optimization Platforms](https://sp-edge.com/industry/128))
4. Platforms for managing other aspects of a firm’s operations such as HRM, payroll, and employee experience (covered under [Remote Work Infrastructure](https://sp-edge.com/industry/15))
5. Platforms for tracking and managing corporate employee expenses (covered under [Business Expense Management](https://sp-edge.com/industry/76))
6. Platforms for providing data security for sensitive data on a firm’s cloud infrastructure and cloud-based applications (covered under [Digital Privacy Tools](https://sp-edge.com/industry/34))

### 

### **Demand drivers**

### **The popularity of the SaaS model, leading to an explosion in the number of SaaS apps**

### 

Traditional software distribution models at firms typically require on-premise installations, have lengthy contract commitments, and require technical knowledge. In contrast, SaaS-based applications are deployed remotely on the cloud, providing flexible payment plans and ease of use.

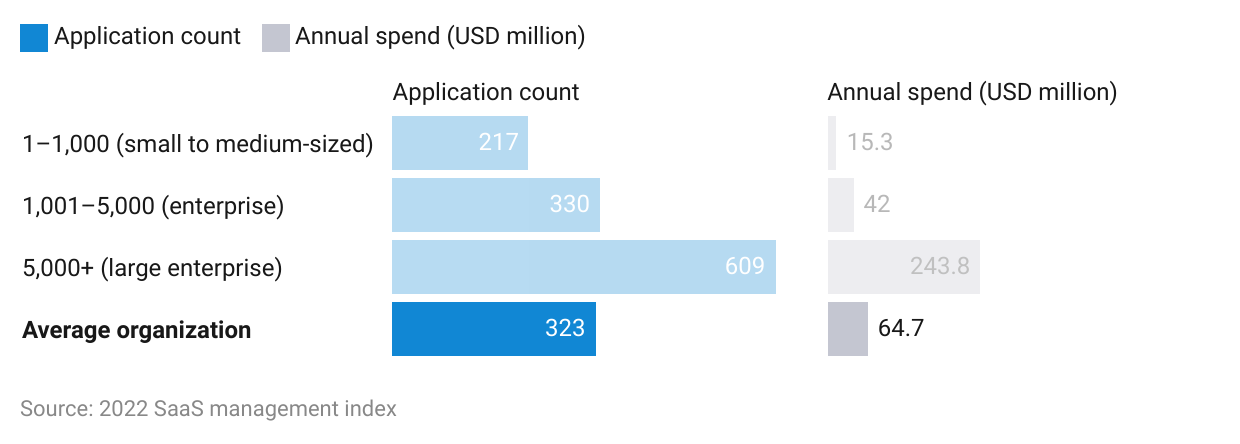
### **Traditional vs. SaaS-based applications**

|  |  |  |
| --- | --- | --- |
|  | **Traditional software applications** | **SaaS applications** |
| Distribution & deployment | **On-premise**  Installed at firm's physical location | **Cloud-based**  Hosted remotely on the cloud |
| Learning curve | **Steep learning curve**  Requires specialist knowledge to deploy and use | **Easy to use and non-technical** |
| Business model | **Expensive**  Lengthy contract commitments  Additional expenses on maintaining the physical infrastructure | **Affordable**  Subscription and licensing basis with free trial periods |
| Scalability | **Lengthy deployment**  May require additional hardware installations  Upgrades to existing systems require physical intervention | **Fast deployment**  Instantly scalable in terms of the number of users and solutions provided  Upgrades to existing applications are done remotely |
| Security & compliance | **More secure** for storing private information  May not be compliant with regulations and data protection policies | **Less secure** for storing private information  Applications are more likely to be compliant with regulations and data protection policies |
| Switching costs | **High**  Lack of interoperability between different applications | **Low**  Ability to integrate different SaaS applications via APIs |

### Source: Compiled by SPEEDA Edge

This has contributed to a steep growth in its popularity, and, as of 2022, the SaaS industry is estimated to be worth more than [USD 170 billion](https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud) and has experienced 5x growth since 2015. This has led to significant growth in spending by firms on SaaS applications as well as the number of apps used by firms of all sizes, with [~80% of firms](https://99firms.com/blog/saas-statistics/#gref) reporting that they use at least one SaaS application.

### **Steep growth in SaaS popularity**

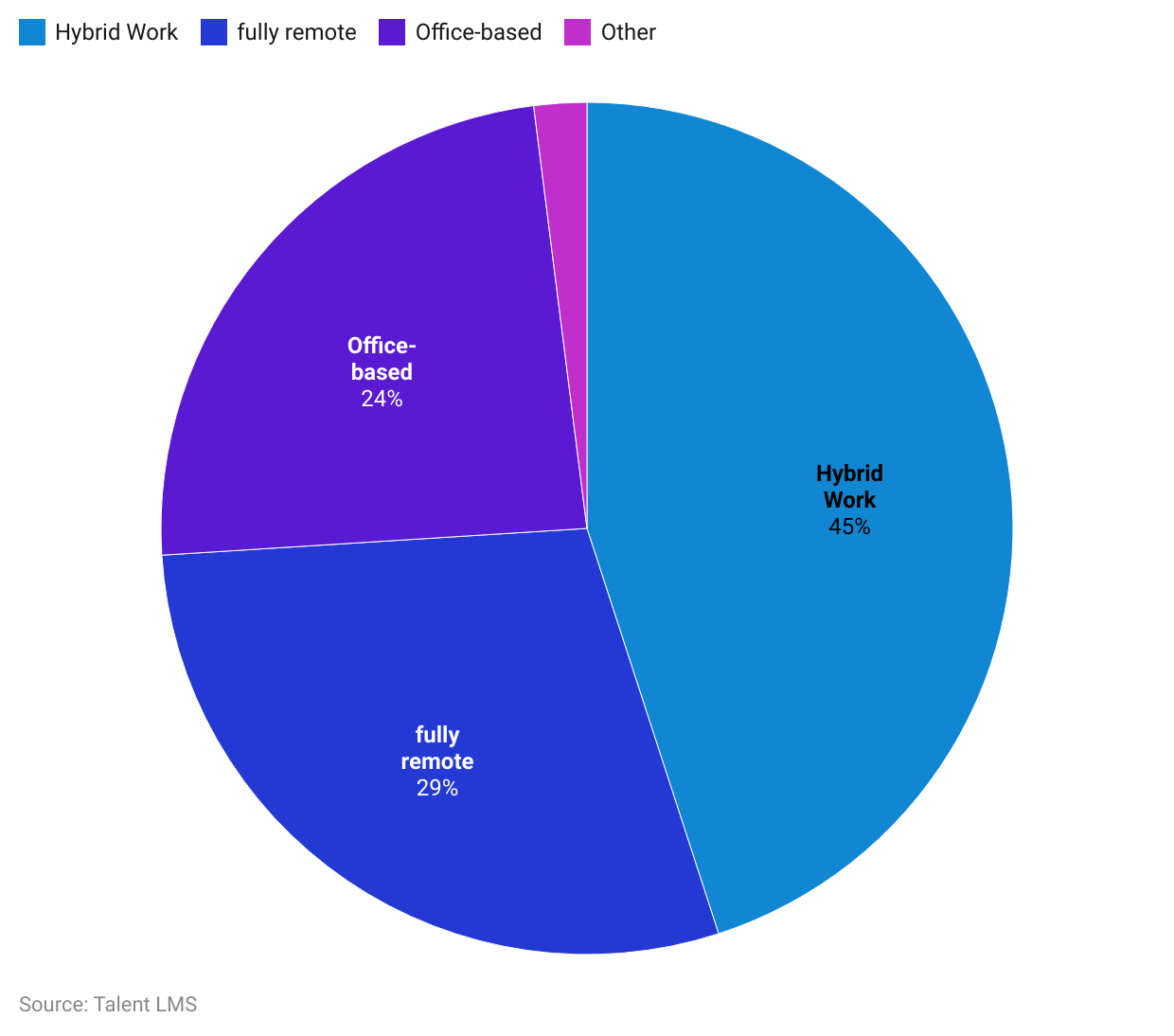


This in turn has created a need for tools to help manage a firm's SaaS stack that is consistently growing. B2B SMPs can help firms with tools to discover and categorize apps while finding the best fit for the firm's needs in a cost-effective manner.

1. **Rise of hybrid working culture, leading to more business processes moving to the cloud**

With the onset of the Covid-19 pandemic in 2020, many employees were compelled to work from home, leading many firms to adopt processes for managing geographically dispersed teams. Even as the threat of the pandemic subsided, [surveys](https://globalworkplaceanalytics.com/global-work-from-home-experience-survey#:~:text=About%20the%20Global%20Work%2Dfrom%2DHome%20Experience%20Survey&text=1)%2073%25%20say%20they%20are,19%20(69%25%20globally).) showed that 76% of employees say they prefer to work from home. This is particularly the case with Gen Z workers who [value flexibility in their work arrangements](https://www.bankrate.com/personal-finance/job-seekers-survey-august-2021/#flexible). In response to both employee needs and potential benefits in terms of productivity and cost savings, many firms including global enterprises such as [IBM](https://www.businessinsider.com/ibm-ceo-hybrid-remote-work-for-most-employees-post-pandemic-2021-3), [Microsoft,](https://www.bloomberg.com/news/articles/2022-03-09/microsoft-s-return-puts-focus-on-workers-who-are-skipping-office?leadSource=uverify%20wall) and [Google](https://www.cnbc.com/2021/05/05/google-relaxes-remote-work-plan-will-let-20percent-of-employees-telecommute.html) adopted hybrid or even fully remote working models. This increased incidence of remote and hybrid working arrangements led to a greater need for cloud-based SaaS solutions. Reflecting this trend, between 2020 and 2022, [global spending on SaaS-based solutions nearly doubled](https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud) to USD 121 billion in 2021 from USD 64 million in 2020.

### **Gen Zers prefer to work on the cloud**



This in turn leads to the growth of Shadow IT and opens up potential security gaps such as data leaks due to information stored on employees' personal devices, loss and theft of devices, and use of unsecure networks for information sharing. In addition, it has led to an increased incidence of processes relating to employee onboarding and offboarding of IT systems to take place remotely. Hence, users of SMPs such as [Torii](https://sp-edge.com/companies/593188), which provide shadow IT discovery solutions to identify and optimize app usage as well as automated remote employee onboarding solutions, claim that it results in a streamlining of its SaaS applications and results in savings in terms of time and money.

1. **Gen Zers want the freedom to bring their own apps to work**

Apart from flexibility in terms of where they work, Gen Zers also place a greater emphasis on the type of workplace tools they use. A [survey](https://www.entrust.com/digital-security/c/shadow-it) of employees indicated they were more productive when allowed to use their preferred applications, and 80% said that their organizations must deploy tools that employees suggest, while [42% of millennials threaten to leave a company](https://blog.toriihq.com/what-should-it-know-about-millennials) due to substandard technology. While enabling employees to use their own apps comes with some risk, it has been shown that organizations that provide greater flexibility and demonstrate a willingness to adapt to employee needs experience lower employee turnover and increased productivity.

Hence, recognizing the value brought by employees from using different apps, SMP platforms such as [Trellica](https://sp-edge.com/companies/853537) follow a collaborative approach, where it provides user engagement tools to understand user behavior and discover opportunities to bring strategic apps into the business.

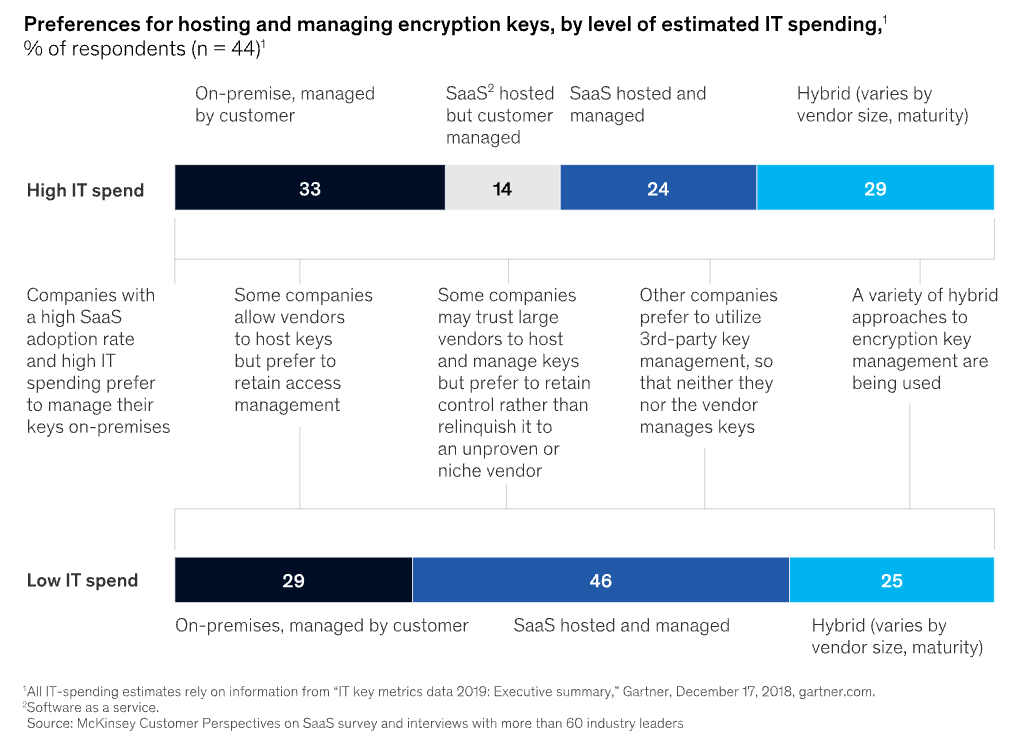
### **Risks and challenges**

**Cybersecurity risk remains a concern for SaaS adoption**

While SaaS applications offer a range of benefits over traditional on-premise solutions, the cloud-based nature of SaaS applications presents an inherent risk in the form of cybersecurity-related threats, potentially leading to the loss of sensitive data and identity theft. This is particularly pertinent in light of the increased focus on consumer privacy and data security, which has led to a plethora of regulations such as HIPAA, GDPR, and CCPA coming into effect around the world and being ever-evolving. Together with stricter enforcement of regulations, which has resulted in high-profile fines such as Google’s [EUR 50 million GDPR fine](https://www.advantage.co.uk/intelligence-hub/check-the-tech/google-set-for-record-50-million-gdpr-fine#:~:text=Google%20have%20recently%20been%20fined,Data%20Protection%20(GDPR)%20rules.), firms have identified this as a significant risk to a firm's operations. This challenge is heightened with respect to SaaS applications, as firms are reliant on vendors to ensure that their applications are compliant with the latest regulations although firms still bear the responsibility for safeguarding sensitive data. Compounding this problem is the fact that many SaaS firms lack transparency with respect to where their data are located and how they are secured.

As a result, many large enterprises opt to secure their sensitive data on-premise instead of on the cloud. This constitutes a limiting factor for greater SaaS adoption with respect to certain business functions such as the collection and storage of consumer and other sensitive data.

**Only 24% of large enterprises trust SaaS providers with sensitive data**

****

*Last updated: December 2022*

©2024 Uzabase, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Uzabase Inc. and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Uzabase Inc. nor its content providers are responsible for any damages or losses arising from any use of this information.