



Buying Software as a Service

TEN KEY QUESTIONS FOR SAAS VENDORS

Executive Summary

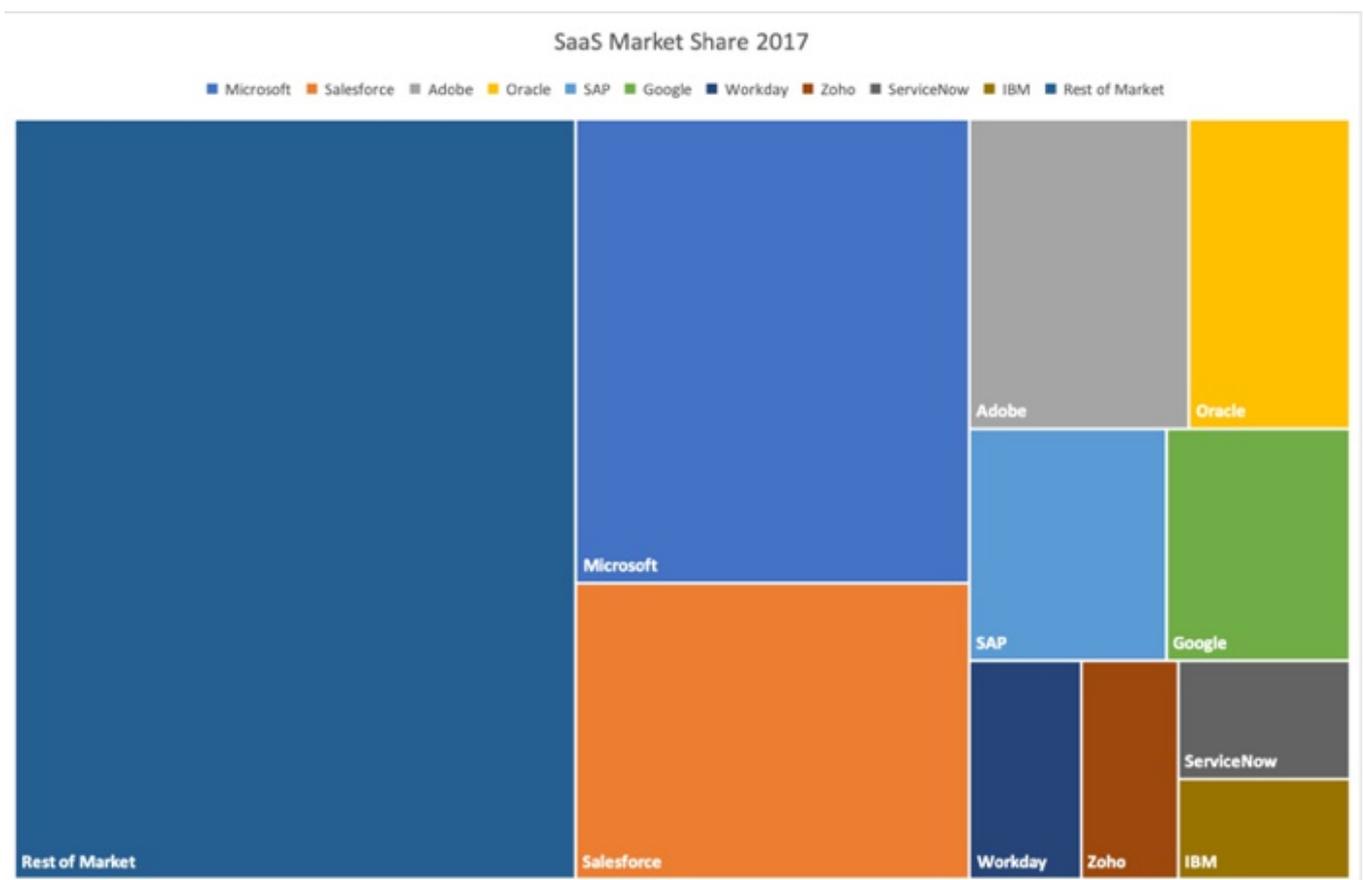
SaaS spending is growing rapidly. By 2020, it will overtake spending on on-premises, perpetually-licensed software. SaaS is mainstream and here to stay. This eBook outlines what's different about buying SaaS, and ten key questions you need to ask to ensure your company receives the full benefits of your investment in software subscriptions.

The SaaS Market

SaaS expenditure has been growing for the last 20 years. Salesforce, 20 years old in 2019, generates almost \$11 billion in annual sales. They've posted annual revenue growth in excess of 20% every year for the last ten years, bar 2009 when the economy was in the grip of the worldwide financial crisis.

The market is expected to grow annually by 20% for the next five years, with total spend approaching \$113bn by 2021 and \$185bn by 2023.

This growth is reflected in the average spend per employee. SaaS optimisation vendor Blissfully report this to be almost \$3000 per employee annual spend. This represents a fundamental shift in the cost of doing business compared to perpetually-licensed software.



Buying SaaS – what’s different?

Whilst the objective is the same (getting the right tools for your employees to do their jobs), the way we get there with SaaS differs compared to perpetual licensing. First and foremost, we’re buying subscriptions, not perpetual rights to the software. This impacts budgeting, forecasting, and accounting practices.

Opex not Capex

SaaS subscriptions are rarely treated as assets. They’re not depreciated, and we can’t “sweat” them. If we don’t pay the monthly or annual charge, we lose access to them. We don’t own anything beyond the right to access the service for the duration of the contract. For this reason, SaaS subscriptions are usually treated as Operating Expenses (Opex), not Capex.

This has a trickle-down impact in a number of areas.

Budgeting & Forecasting

Firstly, your budgeting needs to account for the shift in expenditure. Secondly, your forecasts, particularly for new projects, need to take into account multi-year costs in order to accurately calculate TCO, NPV, or IRR.

Renewals & Maintenance

SaaS applications are continually updated, and with nothing to install, new features and fixes are made immediately available. But you no longer have the choice to cease annual maintenance coverage as you did with perpetually-licensed software. You also lose a degree of leverage with the supplier, as you no longer have that maintenance renewal card to play in contract/renewal negotiations.

Governance

SaaS differs in that generally there is nothing installed on your users’ devices. This makes asset discovery problematic, particularly as much SaaS expenditure takes place outside the traditional IT procurement process, existing as Shadow IT on departmental budgets and expense accounts. With nothing to install and only an internet connection required to access the service, there is a loss of governance with SaaS deployments that increasingly, as a result of the changing legal, regulatory, and compliance landscape, leaves you at risk of non-compliance.



Ten Key Questions for SaaS Vendors

With the above points in mind, what do we need to consider when sourcing SaaS applications? This section groups some key requirements into areas of Security, Service, & Cost.

Security

Security should take precedence over all other considerations. You're putting critical business processes and data into a publicly-accessible network. If you were running a factory, you wouldn't leave it unlocked all night or allow anyone to use the production line. SaaS is now the means of production, or value creation, and needs the same locks and keys as your physical assets.

1. Application Security

SaaS applications remove many of the physical security barriers that protect on-premises software and data. Application Security should be at the forefront of your decision-making process. Key capabilities to look for include the ability to integrate with Single Sign On (SSO) providers such as Okta or OneLogin. And, with almost 90% of former employees retaining access to some cloud accounts after leaving, the service should enable automated onboarding and offboarding of accounts. Finally, at a minimum, the service should offer multi-factor authentication to protect against common cyber-attack methods such as password-spraying.

2. Data storage location

Where is your data being stored? Does your supplier provide this information? Do they meet the regulatory standards required by your organisation? For example, SOC2 compliance, or HIPAA, or GDPR? It is vital to establish this before you start using the service.

3. Supply Chain Security

It is common for SaaS solutions to make use of open source code, also referred to as libraries or dependencies. Ask the SaaS provider to declare whether their product contains open source code, and research the quality of those libraries – this is known as Open Source Code Hygiene. For an idea of what can go wrong see our articles on data privacy breaches at Ticketmaster and British Airways. BA are currently appealing against a £183m fine for their data security breach in August 2018.

Service

The final “S” in SaaS is Service. You’re putting trust in a vendor to provide you with a service that’s fit-for-purpose. These are the things you need to consider from a service delivery perspective.

4. Service Availability

SaaS is usually hosted online with no locally-installed components. Your access to the service is contingent on a number of factors, any of which can make the service unavailable. Critically, more of these factors are outside your control in comparison to a service installed in your local datacentre. Ask your SaaS provider for information on uptime and resilience, particularly for critical business services. Furthermore, work with your Business Continuity Planning team to map out the impact of downtime of a SaaS service and research alternative solutions. Ensure that you agree a Service Level Agreement along with an uptime guarantee for critical services delivered via SaaS.

5. Vendor Viability

The SaaS market is characterised by rapid innovation and a dash to acquire sufficient subscribers before funding runs out. Assessments of vendor viability are important, particularly if they provide a niche capability not readily available elsewhere in the market, or if you are basing a critical business process on a SaaS service.

Failures and acquisitions are commonplace. Acquisitions often result in services being terminated, sometimes at short notice. For example, Twitter acquired content filtering service Smyte in 2018 and immediately shut it down, leaving a number of customers with existing contracts without a service. Microsoft, IBM, and Google have also done this when acquiring services, and all have a track record of sunsetting their own services with limited notice.

Will the service you are relying on be in business for the duration of your contract?

6. Service Catalog

SaaS lends itself to stitching together multiple applications to provide a service. For example, you may use Google Calendar, Calendly, and Zoom to provide a web conferencing service. Build a Service Catalog, highlight the interdependencies of the business objectives enabled by your SaaS environments, and categorise them by criticality, just as you would for on-premises software.

7. Network Performance

Ask the supplier for information regarding required network speeds for your organisation size. A slow network will impact the value you get from SaaS tools, particularly those for real-time collaboration services such as chat and online meetings. If you're in Australia and your service is hosted in an Amazon Web Services datacentre in Virginia, you'll experience poor performance. Similarly, if you are an international organisation, ensure that you carefully select the location for your SaaS tenant. Often services can only be hosted in a single geographic location, meaning that a location central to all users will be most appropriate. For example, in Western Europe Frankfurt is often used as a hub for pan-European tenants.

Cost

For all organisations it is important that services provide value for money, and cost control is a component of this. Here are some aspects of SaaS you should consider from a cost perspective.

8. License Terms

Whilst much SaaS software is licensed on a per-user basis, there are a wide range of metrics used to calculate usage. Make sure you understand the impact of changes in these metrics and that they meet your use case. Be particularly wary of metrics that push you into higher price bands as you grow. Economies of scale do not always apply to SaaS – in fact in many cases the reverse is true. Salesforce is a prime example.

9. Pricing

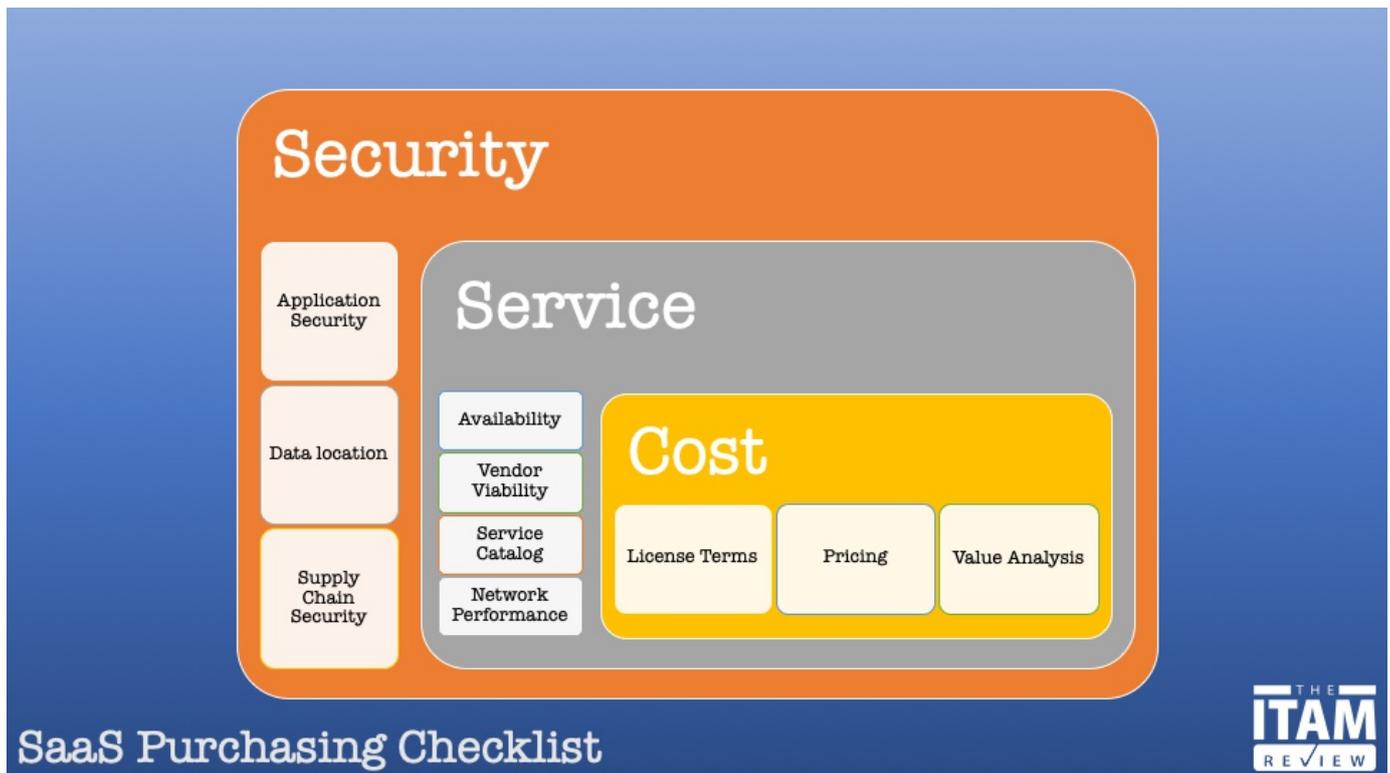
Pay attention to pricing tiers and the features enabled at each tier. Be mindful that SaaS contracts are often short-term, and feature migration between tiers is outside your control and may result in the need to purchase a higher-cost tier in the future. If you intend to use a service long-term, pursue price and feature holds with your supplier to mitigate this risk.

10. Value Analysis

SaaS potentially enables tools and solutions to be more closely aligned with business requirements in comparison to on-premises IT. For example, procurement may use a SaaS service for managing bids. This enables analysis of the value of a solution to the business – it may improve productivity and accuracy and result in cost savings. Dedicated or niche solutions may appear expensive on the surface but yield considerable value for your organisation.

Conclusion

The move to SaaS presents an opportunity for IT Asset Managers to deliver greater value to their organisations. Far from being the “death of ITAM”, it makes the core competencies of our teams – working with software publishers, understanding our IT estate, getting the right deal for our organisations - even more relevant. We have the opportunity to act strategically and deliver considerable expertise to our colleagues in IT Security, Procurement, and Finance. With Digital Transformation seemingly driving business investment in IT for the foreseeable future, we have the opportunity to ensure that journey is one of safety, cost-effectiveness, and value generation.



Further Reading

A major article series, written in collaboration with sponsors Aspera, is accessible here;

<https://www.itassetmanagement.net/2019/04/18/get-to-grips-with-cloud-spend/>

For guidelines on SaaS Security see the NCSC framework at

<https://www.ncsc.gov.uk/collection/cloud-security>

The ITAM Review will continue to research this topic.

Our content collection is here

<https://www.itassetmanagement.net/?s=SaaS>

