Taming the Monster

Managing SaaS in a Fast-Growing Company

AMPLIPHAE

Enterprise IT Evolution

A Cambrian scale

For archaeologists, one of the most exciting times in pre-history was the Cambrian Era, which began about 540 million years ago. At that point, life had existed on Earth for 3 billion years, slowly and steadily evolving into more complex plants and some animals.

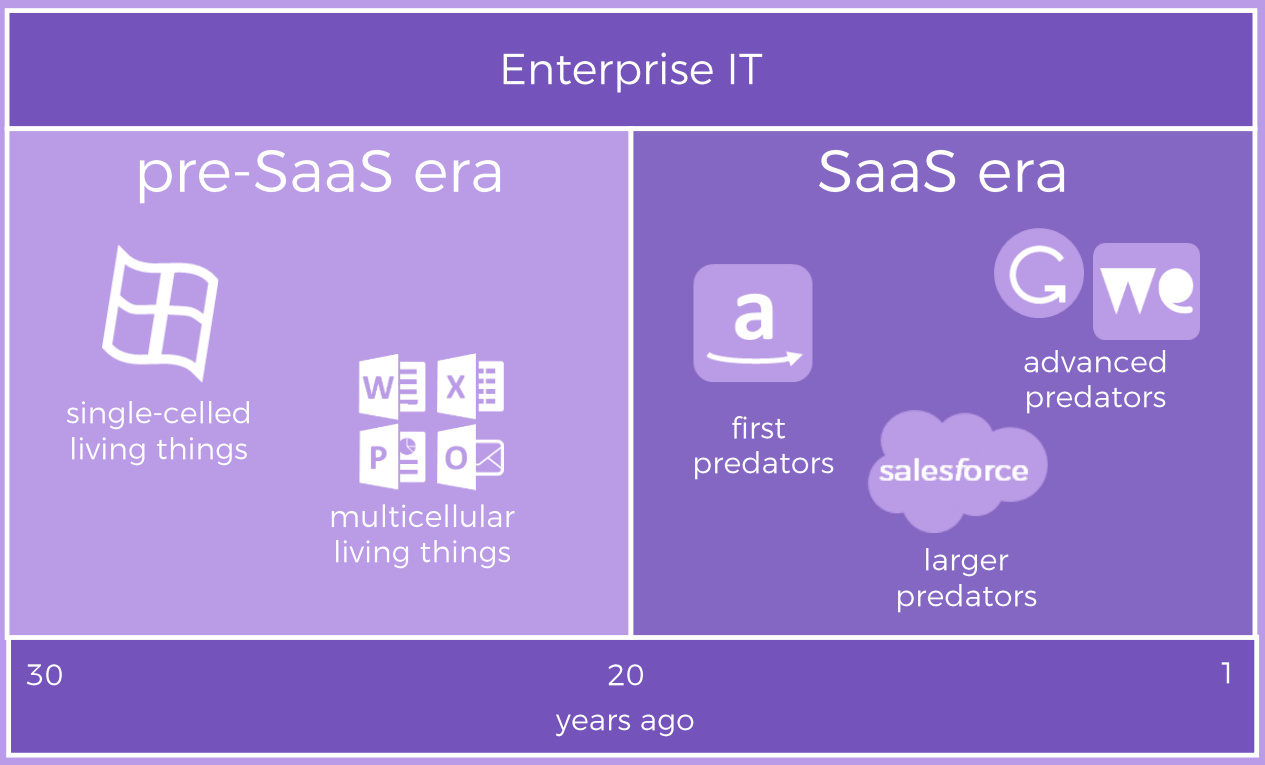
But then something (no-one really knows what) changed in the environment, that prompted a massive increase in the diversity of life. Archaeologists call it the 'Cambrian Explosion' because of the incredible rate at which billions of new species emerged, filling every ecological niche across the planet. It was the end of the era of simple life, and the start of the burgeoning ecosystems we know today.

In enterprise IT we are in the midst of our own Cambrian Explosion, caused by a relatively simple yet profound change in the IT environment, and it's on course to fundamentally change the way organisations consume and manage their application infrastructure.

The era of private, locally managed enterprise applications is nearing its end, and they are being supplemented (and eventually, replaced) by huge numbers of rapidly evolving "Software-as-a-Service" (SaaS) applications. In this deceptively simple change to the established delivery model, the software vendor does not ship packaged software to the customer, but instead runs it themselves in the Cloud, and makes the capabilities available to the customer as a managed service.

Virtualisation – a simple concept with profound implications

At its most basic level, computer virtualisation is a simple concept, that has ultimately had profound and wide-ranging effects on industry and society. The ability to create 'virtual machines' to run application software instead of requiring new physical servers to be bought, installed and managed,



created the conditions that led to Cloud computing – which has reached over $250B in revenues in 2020, with double-digit annual growth for the foreseeable future (according to Gartner).

Cloud disrupted the economics of computing in a fundamental way, and we are still seeing the effects of that shake out. Just like living organisms in the Cambrian, the most agile and innovative players have been ahead of the race to exploit the disruption of Cloud, and what we have seen is an explosion in the number and variety of SaaS applications being brought to market – tens of thousands of applications in just a few years.

Cloud removed the barriers to entry into the global software application market, so that one person with an idea could bring an application to market with literally no up-front investment in computer hardware, scale it from one user to millions without any infrastructure upgrades and offer it to a global audience from the very first day. And now that it's rolling, the mainstream enterprise software vendors have jumped on the SaaS bandwagon as well. For most organisations, the primary way in which they consume Cloud is via SaaS applications, rather than running their own applications in public Cloud.

The rotation away from 'classic' enterprise software, installed and carefully tended by in-house IT experts, to SaaS-delivered applications is now an overwhelming reality for every organization.

A generational opportunity

According to Gartner, SaaS spend will reach $104B in 2020, already represents one-quarter of the whole global enterprise software market and is growing faster than the rest of the market.

The disruptive effects of the SaaS business model offer a once-in-a-generation opportunity to overhaul the way that IT is consumed and exploited within business operations – and some far-sighted organisations have already enthusiastically adopted the SaaS model.

SaaS-first application strategy brings major benefits

The financial benefits of shifting from capital expenditure to pay-as-you-go operational expenditure are clear – it smooths out the application budget and allows delivery of a more dynamic and flexible set of application capabilities for the business. The organisation is not quite so 'locked in' to an application or software vendor in the longer term.

It also allows the organisation to move away from managing infrastructure, which is probably not core business. The management of physical or Cloud infrastructure to achieve the high levels of reliability and uptime that businesses require is a significant challenge, involving investment in expensive staff and management software.

The SaaS model of software ownership also removes other hidden costs from IT operations. Support costs are much lower because the vendor looks after day-to-day maintenance and problem investigation. The customer does not need to spend time testing, planning and deploying application patches and fixes. The vendor is in complete control of software licenses, which means that there is no longer a need for expensive and disruptive software audits by the vendor, which were a much-despised reality of owning classic enterprise software in the past.

The model for SaaS is almost always multi-tenant – where each customer accesses a virtual private copy of the software, but every copy is identical. This removes the temptation to spend significant amounts of money on professional services to customise the software – and thus prevents the business from being locked in to older versions of the application, unable to upgrade without a major investment in

migrating to the new version. With SaaS, every customer is always on the latest version, there is no delay in getting access to the latest features, and no need for professional services outlay every new release.

A SaaS-first approach to IT is also very aligned with Digital Transformation goals – SaaS is where most of the innovation is happening, as it allows small agile companies to bring highly innovative solutions to market quickly and iterate fast. Multiple reports from the likes of McKinsey, PTC, Forbes, and IDC have concluded that use of SaaS is a key success factor in Digital Transformation projects.

The lifecycle of SaaS applications has different dynamics, and we need to adapt our processes to suit

Why is this important?

On the surface, SaaS looks like a relatively simple change in how software is delivered – it is still software, it just runs somewhere else, right? But in fact, the implications for enterprise IT are fundamental and far-reaching. SaaS requires a different approach at almost every touch point, from how it is selected, budgeted for, and procured, to how it is used, managed, and operated, to managing the new risks that SaaS brings to the business.

However, the adoption of SaaS within an organisation does require significant changes in the IT operating model, and is not something that should be left to chance. It is essential to take management of SaaS applications seriously, and existing procedures will need to be adapted to ensure success.

Adapting to SaaS within the enterprise IT stack starts with understanding that the way in which SaaS enters the organisation can be radically different than traditional packaged software. The end-user within a business team is much more involved in SaaS applications onboarding than has traditionally been the case.

The SaaS consumption model brings disruptive benefits, shifting focus away from building and operating data centre infrastructure to instead focus heavily on the application functions needed by the business.

By removing the need to specify and build infrastructure, perform installations and work through procurement processes, teams and individuals feel empowered to make independent decisions about the right applications for their personal use, and bring them into the organisation without reference to any governance procedures at all. While that is great in terms of business agility – and has been the cornerstone of many very successful digital transformation projects – it may leave the organisation exposed to a much greater degree of risk.

Classically, application procurement is a lengthy process – multi-year agreements for sprawling application suites delivering broad value across multiple business functions. That process starts with the business teams specifying their requirements to support operational needs; project scope and specifications are drawn up; and an application is either sourced or custom-developed in line with the existing enterprise architecture. The IT team takes into consideration key requirements like regulatory compliance, security, privacy, business continuity, service management and long-term IT strategy. This process is reliable and delivers good governance of application software, but it is not a fast process and often causes friction between the business teams and IT due to a in expectations about the velocity at which applications can be made available.

Figure 1: Lifecycle Model for Centrally adopted Applications

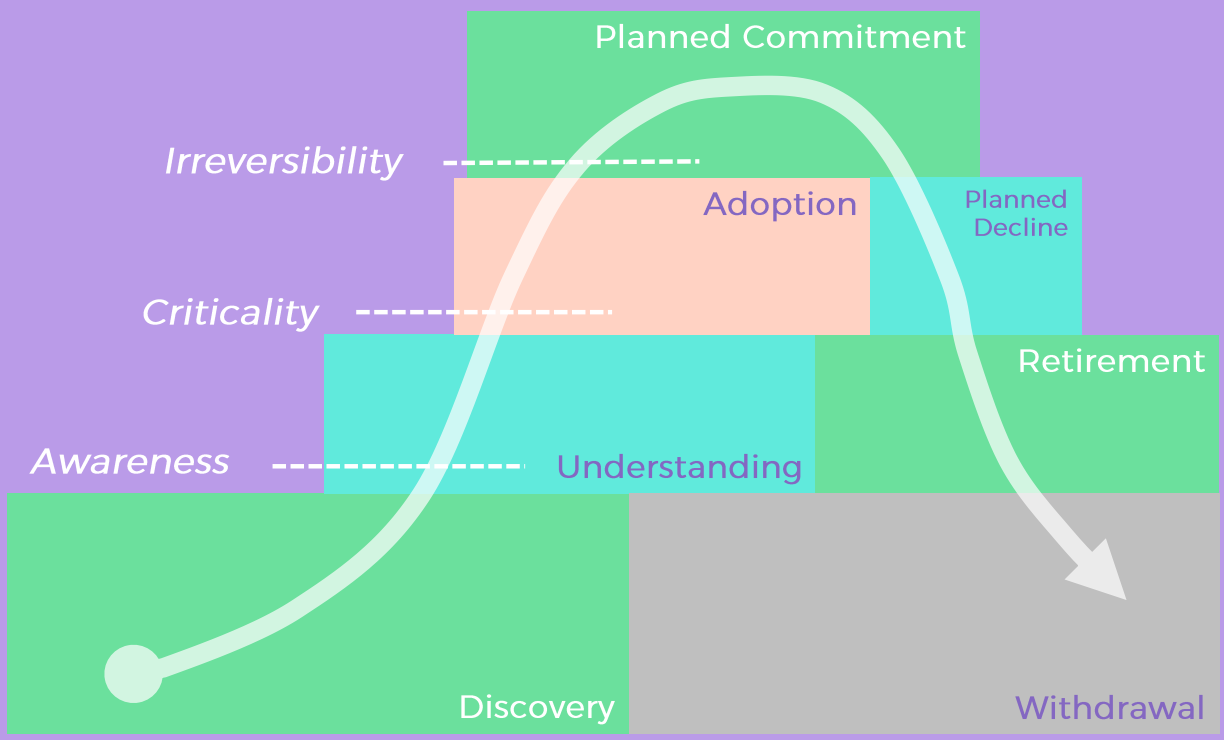


Figure 1: Lifecycle Model for centrally adopted applications

Figure 1 shows a lifecycle model for how a classic locally managed application is introduced into the organisation, becomes mainstream, and is eventually retired from service in a planned way. Onboarding a new application into the organisation begins with a discovery period as decision makers encounter an application for the first time and raise awareness amongst stakeholders within the organisation. At this point the organisation is aware of the application and actively working to decide how to proceed. A controlled assessment is carried out (across all functions, i.e. technical, commercial, etc.) leading towards a decision to either adopt the application or decline to do so.

Eventually, once the assessment team has given the go-ahead the application is rolled out within the organisation, becoming critical to the operations of some parts of the business and eventually the business becomes committed to the application – often crossing an 'Irreversibility Threshold' at which stage it becomes difficult to remove the application from the organisation without significant effort.

The lifecycle for user-driven SaaS adoption is potentially very different – see Figure 2.

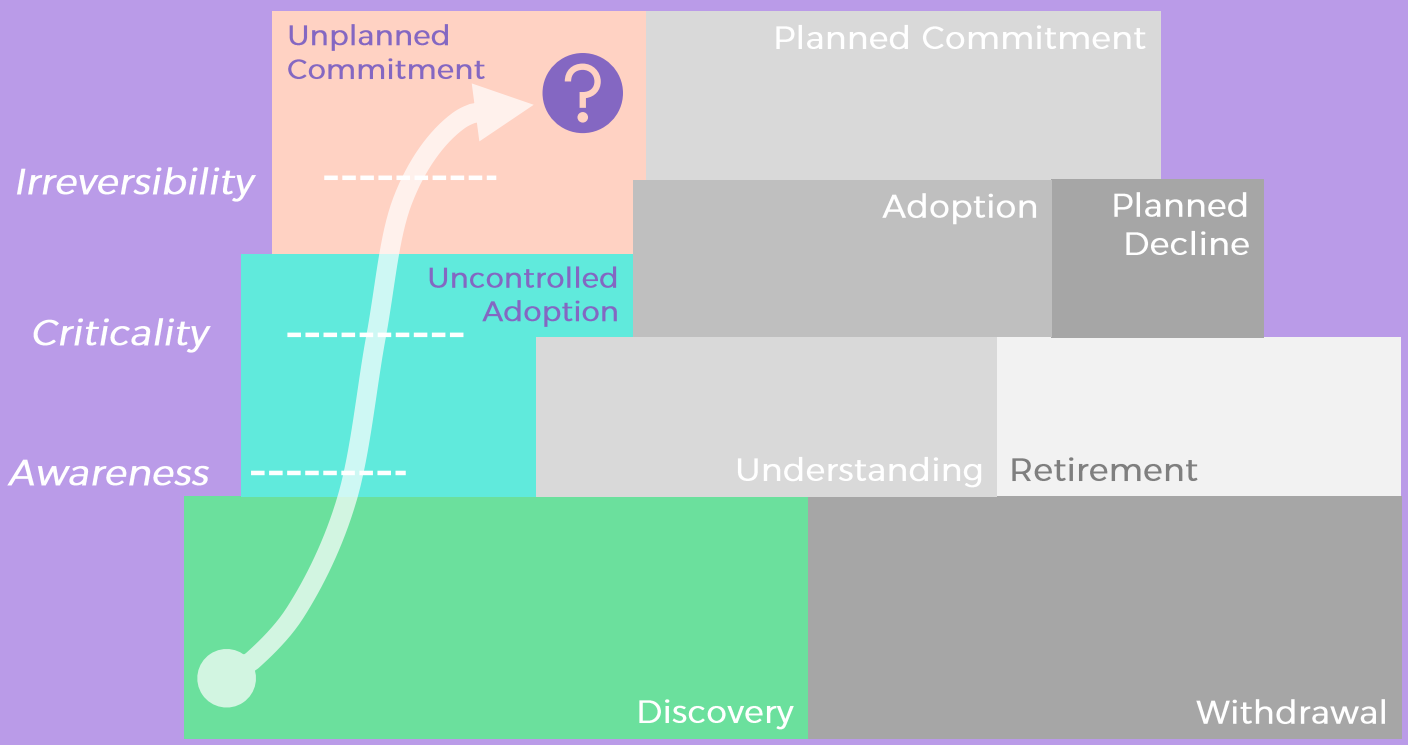


Figure 2: Lifecycle model for user-Adopted SaaS

In this model, the SaaS application is brought into the business by an individual, not IT, and spreads virally across the organisation. Such adoption is built into the business model of many SaaS applications, with two-minute user sign-up and encouragement to introduce colleagues via email addresses.

The SaaS application can rapidly spread without IT oversight and rocket through the criticality and irreversibility thresholds before anyone has had a chance to apply due diligence. At that point, the organisation has become committed to the SaaS application, it is embedded in working practices and it will be disruptive to remove it. If a commercial or security exposure is uncovered, making the application incompatible with the organisation's policies, it will be a major task to back out.

The SaaS business model has a big impact on how applications are consumed by an organisation, but what are the implications of that on IT operations? In fact, the impacts can be quite profound, especially if the people within the organisation begin to enthusiastically adopt highly domain-specific SaaS applications to help them with their local business processes.

SaaS requires IT operational processes to be adapted.

Why?

SaaS changes the procurement dynamic for software.

The relationship with the software vendor is radically changed.

The organisation will need to deal with many more vendors.

SaaS applications make privacy compliance more complex

The risk profile for the organisation will change.

Cloud applications do not solve all security & continuity problems

The enterprise architecture is much more complicated.

Procurement

With dramatically simplified on-boarding (no servers required, no installation) and a lower up-front investment due to month-by-month payments, maybe on a credit card, individuals and teams are empowered to choose and use the applications they feel meet the needs of their business processes. The IT team will still coordinate the procurement of the core mainstream applications (think Microsoft 365 or Salesforce) but for the vast majority of SaaS, the line of business will not feel the need to involve IT.

This effectively democratises the decision-making process around software, much more so than for classic locally-managed applications – and can lead to a loss of control over software budgets. With individuals and teams making independent decisions, there is a strong potential for duplicated spending, with lost opportunities to consolidate all the spending with a vendor and thus negotiate better pricing. The fact that spending can happen through many routes including departmental budgets, shared corporate cards, personal credit cards and expenses – instead of a traditional purchase order and invoice – adds to the potential for uncontrolled spending.

Without good, centralised awareness of the SaaS applications in use and coordination between departments and end-users, it is very difficult for the organisation to develop an understanding of the overall SaaS spending, and control it effectively to make best use of budgets.

Vendor Relationship

The relationship is changed and deepened when software is delivered as SaaS. In the past, software was delivered by the vendor and then operated by the customer, and the ongoing dependency on the vendor was at relative arms-length, consisting mainly of support and regular patches and upgrades, perhaps some training or professional services.

With SaaS no software is delivered, instead the vendor operates the service day-to-day on behalf of the customer, and the customer's data is held and processed on vendor infrastructure and under vendor control. With limited direct control or even visibility behind the SaaS curtain, the IT team do not directly control the software and by necessity must take on more of a 'hands-off' governance and compliance role on behalf of the organisation.

The change in vendor relationship is quite profound and leads to the need to assess the SaaS application and the vendor in a much more thorough manner than for delivered software.

Number and Type of Vendors

The disruptive economics of Cloud mentioned above means that SaaS applications are often very focussed on a small set of functions. With classic enterprise applications, high fixed costs (of customer acquisition, distribution, support, etc.) meant that there was an advantage to both the vendor and the consuming organisation in combining many functions into a suite of software, sold under an all-you-can-eat enterprise-wide license. That acted to exclude other smaller players. But SaaS levels the playing field so a micro-scale software vendor can launch and successfully support an application that focusses on doing only one thing – but probably doing it well.

So instead of a few tens of enterprise applications managed by in-house IT, delivered by a few monolithic software vendors, the organisation will have hundreds or thousands of SaaS applications in regular use, many of them niche and used by only a small subset of their people.

This radically increases the workload in several key processes, such as vendor risk assessment, subscription renewals and employee on- and off-boarding. It may require as much or more effort to work with a micro-vendor with a few employees, as it would to work with a major vendor like Microsoft, IBM, or Adobe – because the small vendor is likely not geared up to deal with enterprise processes.

It is also extremely likely that the IT team will not have a good view of what applications are in use across the organisation, since they were not involved in choosing or acquiring many of them. The task of discovering the SaaS that has been brought into the organisation can be significant, even before those applications can be brought inside of formal governance processes.

Privacy Compliance

Privacy legislation is evolving rapidly across every jurisdiction (GDPR in the EU broke early ground but most countries are catching up) and is increasingly critical for every business. The implications of putting your customer data into a SaaS application cannot be understated, and it is absolutely essential to assess every SaaS application with an eye to privacy. Issues such as geographic location of the vendor and the application data are vital and yet often very difficult to assess – as mentioned previously, the nature of SaaS supports small vendors who do not always have the resources to manage complex, confusing and contradictory global privacy legislation.

The ways in which SaaS is acquired can also lead to privacy non-compliance. A key cornerstone in privacy management is contractual management of the data processor – data controller relationship between supplier and customer. In many cases SaaS is transacted entirely online through a web page, and the only contract is a click-through End User License Agreement (EULA) which is emailed to the individual that signed up to the service. It can be immensely difficult for the privacy professional to identify the SaaS applications in use, trace what types of data might be stored in them, and then assess whether the correct contractual protections are in place.

Risk Profile

An application is not necessarily riskier simply because it is delivered from the Cloud on a SaaS basis. But the nature of risk that the organisation is exposed to is different for SaaS – and the compliance and governance professionals in the organisation need to take account of the changing risks across their application landscape.

Since most SaaS applications will be adopted outside IT it's likely that the risk assessment process will at least initially be light or non-existent, as line-of-business professionals are likely to be more concerned with application functionality than compliance. However certain aspects of SaaS do need to be taken seriously, and high on that list is data governance. Since the SaaS vendor operates the application and manages the data on behalf of the customer, the policies and procedures of the vendor are of utmost importance and must be examined carefully.

The reality is that, for many smaller vendors, even when a SaaS application has been identified in use, it can be difficult to determine whether the vendor has taken all the necessary steps to secure and protect the data that they are entrusted with.

Business Continuity & Security

There is a temptation to assume that if a vendor is using a public cloud platform, their application will be inherently more secure and reliable. There is some truth in this, since at the infrastructure layer, the major cloud providers have invested a lot in ensuring best practices are used. However a lot is still left to the application vendor in terms of the application software itself and correct use of the Cloud platform.

SaaS applications are now the single biggest target for phishing and other attacks, so the security of SaaS applications and vendors has to be taken seriously and actively managed, requiring significant effort from the customer. If the vendor has achieved security certifications such as ISO 27001 or SOC 2 that will give some confidence, and the use of tools such as Cloud Security Alliance STAR and Cloud Controls Matrix can help with measuring risk.

Complexity

The set of systems and applications which support every business are becoming increasingly complex and interconnected, and having a robust enterprise architecture is critical to ensure that the IT environment supports business objectives effectively. As different parts of the business independently adopt diverse SaaS applications without strong architectural governance, the overall architecture can become brittle, with multiple applications providing overlapping functions in silos across the organisation. This makes it much more difficult to enforce common policies, move staff around without extensive retraining, or share data between different parts of the business.

As organisation data fragments across many more geographically dispersed SaaS applications, the task of understanding and optimising the interfaces between Cloud applications and legacy on-premises applications becomes extremely complex. Key applications across the business need to efficiently share information to support business processes, and this can be challenging with SaaS applications, where there is limited control over data and interface formats.

SaaS represents a huge opportunity for Enterprise IT,

Like life on earth after the Cambrian, expanding to fill every ecological niche, we are at a point of huge potential benefit for any organisation that fully embraces the SaaS model for IT applications. They can exploit a *velocity of innovation* that has never been seen before, whilst enjoying *flexible commercial models* that directly relate software costs to core business operations. They can *free their IT teams* from tending infrastructure to focus on higher-value tasks like transforming the way they interact with customers and ensuring that business processes run optimally and comply with legislation.

But it has to be managed properly to avoid risk.

But going *all-in* on SaaS can only be done safely with the right underpinnings and processes, and many companies *will struggle* to fully exploit the SaaS Era due to outdated SaaS management.