AXONIUS

Navigating the Complexity of SaaS Management

Introduction.

How businesses consume software has evolved over the years. While cloud adoption is showing no sign of slowing down, software as a service (SaaS) models have become a go-to for many organizations. In fact, the global SaaS market size is projected to reach $307.3 billion by 2026 - a notable increase from $158.2 billion in 2020.[1]

And with SaaS applications - Slack, Google Workspace, Zoom, Salesforce, HubSpot, and so many more - helping organizations pivot to remote and hybrid work and fuel their digital businesses transformation, the appetite for SaaS will continue to grow.

But as SaaS adoption continues to skyrocket, it's also adding more complexity for IT and security teams. The most pressing need? A comprehensive approach to SaaS management.

READ ON TO LEARN:

1. **The key SaaS challenges - including shadow SaaS and SaaS spend – and how they impact security teams**
2. **Current approaches to SaaS management - and their limitations**
3. **Why a modern, comprehensive approach to SaaS management can help**

$145.3 Spending on SaaS services is predicted to reach **$145.3 billion** in 2022[2]

50% The overall spend per company on SaaS products is up by **50%** compared to two years ago[3]

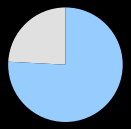
137 Mid-market businesses typically use an average of **137 SaaS apps**[4]

WHAT'S THE SaaS PROBLEM?

The advent of the SaaS model has undoubtedly brought along a major paradigm shift in the history of IT.

SaaS offers organizations several advantages: increased flexibility, accessibility, cost savings, productivity gains, and more.

This shift in paradigm, however, has resulted in an exponential increase in complexity for IT and security teams (think data sprawl and security implications). What's more, it amplified visibility challenges for many organizations. And that's not all.



76% of IT professionals see unsanctioned apps as a security risk[5]

HERE'S A LOOK AT SOME COMMON SAAS-INDUCED CHALLENGES FOR IT AND SECURITY TEAMS:

1. **Getting a credible SaaS asset inventory with complete visibility into known and unknown SaaS apps and intricate data flows**
2. **Managing configuration, licensing, and security gaps across thousands of SaaS applications**
3. **Measuring SaaS application risk and ensuring compliance**
4. **Monitoring SaaS spend**

Compounding these challenges, only point solutions exist for SaaS security and cost optimization.

As businesses accelerate SaaS adoption, a comprehensive solution that addresses risk management and business value for SaaS in one place for all stakeholders is imperative for business success.

SaaS MANAGEMENT: 4 KEY CHALLENGES

As SaaS adoption continues to explode, getting a deeper visibility into SaaS apps within the organization, uncovering the interconnectivity of SaaS apps, understanding security coverage and configuration, and controlling SaaS spend has become more important than ever.

Let's take a deep dive into some of the top SaaS challenges.

INTERCONNECTIVITY AND DATA SPRAWL.

What happens when an organization has a lot of applications in its SaaS stack? SaaS sprawl. And this, in turn, introduces data sprawl.

SaaS data sprawl is the result of the decentralized distribution of information in different applications, making it difficult for IT to answer questions like:

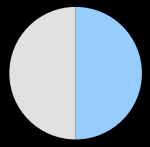
1. Where does all the data reside?
2. Where is sensitive or personally identifiable information (PII) being processed?
3. Who has access to the data?
4. How secure is the data?

Think of an employee who's more comfortable using Google Drive for storage - even when their company uses Box. They go ahead and use Google Drive - but IT doesn't know about it. When they leave the organization, though, the data remains in Google Drive forever. That data then becomes much harder to track down and recover.

Another driver of SaaS sprawl? Open APIs. As they've become a market standard, customers expect all their SaaS solutions to work jointly with one another to drive operational efficiencies.

Take Salesforce, for instance. Salesforce offers a limitless number of supported integrations. Many teams integrate Salesforce with email tools, marketing tools, chat and collaboration tools, and more. This means customer data stored in Salesforce can be easily transferred to any other application - making it hard to keep track of every place the data lives.

The implication? Putting customer data at risk. In a time when compliance mandates like GDPR mean more scrutiny on protecting customer data, unmanaged SaaS sprawl is a risky undertaking.



Up to 50% of an organization's SaaS environment can pose visibility and management challenges[6]

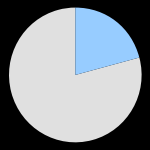
SHADOW SaaS.

Another problem introduced by SaaS sprawl? Shadow SaaS - where employees use SaaS applications without the IT team's knowledge.

In fact, one in three employees at Fortune 1000 companies regularly use cloud-based SaaS apps that haven't been explicitly approved by internal IT departments.[7]

While employees have bypassed IT departments for ages, SaaS usage has introduced another shadow IT opportunity. Why? Because SaaS offerings present unique solutions to address specific user requirements that may not be addressed by an organization's IT solutions.

The convenient purchase process of SaaS apps, including free trials or pay-as-you-go options, is also accelerating shadow SaaS adoption. This makes it difficult for IT and security teams to identify any SaaS app that isn't in use.



21% of organizations experienced cyber events due to a non-sanctioned IT resource[9]

WITHOUT SAAS APPS GETTING THE PROPER SECURITY AND IT REVIEW UPFRONT, NUMEROUS RISKS ARE INTRODUCED.

DATA LOSS

Shadow SaaS can drive unknown attack surface expansion. In fact, 79% percent of organizations identified compromised company data and security information as the top risk of deploying shadow SaaS apps.[8] That's because shadow SaaS apps have bypassed IT's typical vetting procedures. These applications are also less likely to be integrated with user-based security processes. Often, the SaaS providers themselves don't have adequate expertise or measures in place to protect customer data.

COMPLIANCE RISK

Shadow SaaS also makes your organization vulnerable to non-compliance risks. Regulations like HIPAA and GDPR specify how companies can use, store, or transfer consumer data. SaaS providers that fail to comply with these regulations could cost businesses millions of dollars in fines. Plus, some SaaS providers may not hold a SOC 2 certification, or could fail to renew their PCI DSS compliance. Depending on what industry you're in, this could be a big risk.

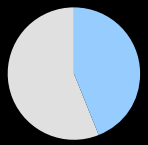
INCREASED COSTS

Beyond security and compliance concerns, shadow SaaS puts strain on business budgets. Spend on shadow SaaS apps may be small in isolation - but at scale, they can drive considerable costs. And when finance and business operations teams don't have line of sight into this spending, budgets quickly become hard to manage.

MANAGING SaaS SECURITY RISK.

Managing SaaS security risk is a time-consuming and complex initiative - even for SaaS applications sanctioned by IT and security teams.

Further escalating the SaaS security management challenge? The fact that SaaS apps are becoming more customizable.



44% of SaaS user privileges are misconfigured[10]

LET'S LOOK AT TWO SPECIFIC PROBLEM AREAS WHEN IT COMES TO MANAGING SAAS SECURITY RISK.

Managing SaaS settings

An average SaaS application has many configurable settings that - if left unchecked - can introduce security risks. Given that enterprises use hundreds or even thousands of SaaS applications, most security teams likely have thousands of settings to manage across all SaaS applications. The frequent updates inherent in SaaS platforms compounds this challenge.

Misconfigurations can make apps publicly accessible, and attackers can leverage weak configuration settings to access sensitive data.

Identity and access management

As SaaS adoption continues to rise, controlling who's granted access to which applications becomes increasingly important. Identity and access controls make up a large percentage of settings that security teams need to manage. But many SaaS users have admin rights or excessive privileges, posing data security risks - including insider threat.

MANAGING SaaS SPEND.

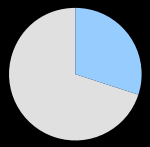
If your organization is spending more than it should on SaaS applications, you're not alone.

As SaaS adoption increases, controlling SaaS application spend is another area of concern for IT and security teams.

The unexpected global pandemic also triggered a massive uptick in SaaS spending. Today, enterprises are spending an additional $20B on SaaS each year.[11]

But tracking SaaS spend across all departments remains a challenge.

Why? Decisions to move forward with renewals and upsells of SaaS subscriptions are often decentralized and made at the department-level.



Up to 30% of SaaS spend is wasted because of under-used, unused, orphaned, excess licenses, and overpriced vendors.[12]

LET'S LOOK AT SOME OF THE AREAS DRIVING SAAS SPENDING ISSUES.

SHADOW SAAS

When employees use SaaS applications without IT's knowledge, the number of SaaS applications in the organization increases. This adds to the SaaS spend.

REDUNDANT APPS

Procuring SaaS applications without checking the existing SaaS stack also increases the overall SaaS spend. Lack of an up-to-date inventory is another key driver for redundant SaaS apps. With scores of SaaS applications in use, it's common for companies to have multiple SaaS applications delivering the same functionality. For example, companies may be using - and paying for - both Google Drive and Box.

EXTRANEOUS USER LICENSES

Organizations risk unnecessary spending if they're not properly monitoring their SaaS user licenses. That's because a lot of SaaS applications charge per user account. Underused or duplicate SaaS licences can result in extraneous costs.

ORPHANED ACCOUNTS

When employees leave a company or change departments, they may still have active accounts with various SaaS apps. Apart from adding to SaaS stack visibility challenges, the most obvious problem with orphaned subscriptions is wasted money on software with no accountable owner.

INACTIVE ACCOUNTS

It's also common that licenses are granted for users, but they don't end up needing or using them. For example, a DocuSign license may be allocated to an employee who doesn't have privileges to sign for contracts. Some SaaS services also charge per user, per month, instead of charging for the total number of projects hosted. The result? Significant increase in costs for businesses with inactive users."

SaaS MANAGEMENT APPROACHES – AND THEIR LIMITATIONS

Ten new SaaS apps get into your company every month.[13] What does this mean for your business? More SaaS complexity affecting people across IT, security, BizOps, and finance teams. While processes for managing SaaS may differ from company to company, technologies have emerged to help teams tackle these challenges in isolation.

SaaS MANAGEMENT PLATFORM.

Another market gaining traction over the last few years is SaaS Management Platforms (SMP). SMPs monitor SaaS tools. They allow IT teams to manage the day-to-day SaaS operations (SaaSOps) and improve employee experience for frequently used SaaS applications. This includes user onboarding and offboarding, tracking application usage, and visibility into licensing and cost optimization.

Some SMPs have basic security functionality built-in, but these platforms' primary use cases cater strictly to the IT management and operations of SaaS applications. They often don't:

1. Provide robust information into SaaS settings misconfigurations, data flows and types, and user access levels - all of which are needed to reduce security risk
2. Detail the security risk level and compliance status of SaaS providers you're already using

SaaS SECURITY POSTURE MANAGEMENT.

In 2020, Gartner named a new category for cloud security - SaaS Security Posture Management (SSPM). SSPM platforms provide automated continuous monitoring of SaaS applications to help security and IT teams minimize risky configurations, manage policies, and ensure compliance.

While the SSPM market is gaining traction, SSPMs often don't:

1. Offer visibility into end-user devices accessing SaaS applications - meaning security teams only get a fragmented view of the whole picture
2. Shed insight into SaaS licensing to help with cost optimization - meaning they aren't useful for finance and business operations teams

CLOUD ACCESS SECURITY BROKER.

Cloud Access Security Broker (CASB) is a software tool that sits between an organization's on-premises infrastructure and a cloud provider's infrastructure. It acts as a gatekeeper between users and SaaS providers, allowing security teams to control how users access SaaS applications.

While the CASB market has been around for 10 years and CASB solutions offer security benefits, it's important to understand its limitations around SaaS management. CASBs often:

1. Only have line of sight into select SaaS applications that security teams know about
2. Take a user-centric approach that doesn't account for the myriad settings within the SaaS applications that may introduce risk
3. Don't help with cost optimization by offering insight into SaaS licensing, and aren't useful for finance and business operations teams

NEED FOR A MODERN APPROACH TO SaaS MANAGEMENT

SaaS offers tremendous value to organizations, but businesses need an easier path to rein in SaaS complexity.
The way forward? Adopting a comprehensive approach to SaaS management that solves IT, security, risk, and finance teams' challenges by giving them a single source of truth into every SaaS application.

A modern approach to SaaS management enables stakeholders to:

1. Discover both known and unknown SaaS applications, providing complete and actionable visibility into all data types and interconnectivity flows. This will allow IT and security teams to gain control over their complex SaaS applications environment
2. Uncover and mitigate various security risks that put sensitive customer and business data at risk - including identifying misconfigured SaaS settings and suspicious or malicious behavior
3. Deliver the insights on user access and app utilization needed for better IT management and cost optimization across all SaaS apps
4. Streamline SaaS compliance reporting

End Notes.

1. "Global Software as a Service (SaaS) Market Report, History and Forecast 2016-2027." Valuates Reports. 2020
2. "Forecast: Public Cloud Services, Worldwide, 2019-2025, 1Q21 Update." Gartner. 2021.
3. "SaaS Trends 2020." Blissfully. 2020.
4. Ibid.
5. "2020 State of SaaSOps." BetterCloud. 2020.
6. "6 Steps to Optimize SaaS Productivity and Security." LeanIX. 2021.
7. "Bring shadow IT into the light: Discover, assess, approve and educate." IBM.
8. "6 Steps to Optimize SaaS Productivity and Security." LeanIX. 2021.
9. "Perception Gaps in Cyber Resilience: Where Are Your Blind Spots?" Forbes Insights.
10. "2021 SaaS Risk Report." Varonis. 2021.
11. "Forecast: Public Cloud Services, Worldwide, 2019-2025, 1Q21 Update." Gartner. 2021.
12. 6 Steps to Optimize SaaS Productivity and Security." LeanIX. 2021.
13. "What is SaaS Management?" Zylo.

See how you can uncover the interconnectivity of SaaS apps within your organization, understand security coverage and configuration, monitor SaaS spend, and obtain a deeper level of visibility into SaaS apps - all in one comprehensive solution.

SEE FOR YOURSELF

330 MADISON AVE., 39TH FLOOR
NEW YORK, NY 10017
info@axonius.com

Axonius gives customers the confidence to control complexity by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies. Cited as one of the fastest-growing cybersecurity startups, with accolades from CNBC, Forbes, and Fortune, Axonius covers millions of assets, including devices and cloud assets, user accounts, and SaaS applications, for customers around the world. For more, visit Axonius.com.