

# Let's Talk SaaS

*A Comprehensive Strategy for  
Controlling SaaS Complexity*



## **Need a way to communicate with your team?**

*There's an app for that.*

## **Help managing tasks or raising productivity?**


*Lots of apps for that as well.*

## **Managing employee information, payroll, and logistics?**

*Yup, that too!*

Slack, Zoom, Google Workspace, Workday, and other SaaS applications are integral parts of how employees work every day. SaaS apps are in practically every department — finance, sales, marketing, human resources, and more. Employees see a lot of benefits with SaaS, like increased productivity, accessibility, and flexibility.

On the flip side, though, come challenges for IT and security professionals (think data sprawl and security vulnerabilities). With employees and teams often working in silos, IT and security typically lack visibility into the company's entire SaaS stack. And without that visibility, it's impossible to ensure that critical data processed by and stored in SaaS apps is protected.





What's needed is a long-term, collaborative, and effective SaaS strategy. One that continues to provide employees with efficiencies, while giving IT and security a single source of truth into the SaaS stack.

But how do IT and security get to this understanding with internal stakeholders like human resources, sales, and customer support?



**Read on to learn:**

- *The SaaS challenges IT and security professionals face*
- *Why SaaS ownership is so complicated*
- *Ways to adopt effective SaaS ownership practices*
- *How a modern, comprehensive approach to SaaS management helps streamline and improve an organization-wide SaaS strategy*


# The SaaS Challenges of IT and Security Pros



*Over the last five years, SaaS app consumption increased dramatically.*

*Right along with it? Increased spending on SaaS.*





SaaS spend accounts for the largest portion of cloud services spend (like, Infrastructure as a Service and Platform as a Service) in businesses, according to Gartner<sup>1</sup>.

In fact, 66% of IT and security professionals spend more on SaaS applications today than a year ago<sup>2</sup>.

As adoption rates continue to surge, SaaS apps introduce a slew of challenges for security and IT professionals to tackle, like:

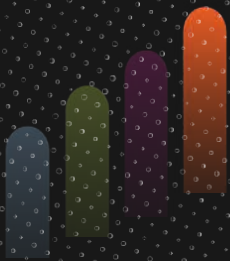
- *Understanding which SaaS apps are being used across the organizations — and if they're all properly managed*
  - *Ensuring employees are properly onboarded and offboarded from applications*
  - *Securing sensitive data stored and shared across the company's SaaS app stack*
  - *Monitoring the compliance of SaaS providers against relevant frameworks and certifications*
  - *Optimizing SaaS spend, rightsizing SaaS licenses, and eliminating redundant applications*
- 

<sup>1</sup> “Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$600 Billion in 2023”. Gartner. October 31, 2022.

<sup>2</sup> “The Truth About SaaS Security and Why No One Cares ... Yet”. Conducted by Savanta on behalf of Axonius. 2022.

Businesses are increasingly looking for easier ways to rein in all this SaaS complexity. An effective, collaborative SaaS strategy is key.

More often than not, this strategy starts with understanding how the SaaS apps are owned within the organization.



- \$195.2B — Projected end-user SaaS spend in 2023<sup>3</sup>



- 74% — IT and security professionals who report over half of their apps are SaaS based<sup>4</sup>

***“As many have learned — some in more difficult ways than others — “the cloud” is just someone else’s computer. Any strong IT asset management strategy must account for assets that aren’t owned or directly operated by the organization itself. This is especially true given that many SaaS providers offer integrations with both SaaS and on-prem services, which may include delegating ongoing access to data or systems to a third party. Ongoing access can become a serious liability if an organization fails to track material changes that could impact its SaaS providers.”***

— Daniel Trauner, senior director of security, Axonius

<sup>3</sup> “Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach Nearly \$600 Billion in 2023”. Gartner. October 31, 2022.

<sup>4</sup> “The Truth About SaaS Security and Why No One Cares ... Yet”. Conducted by Savanta on behalf of Axonius. 2022.



# SaaS Ownership Complications



*For security and IT teams, streamlining SaaS management is filled with obstacles.*

*Mapping their company's SaaS application environment is just one of these stumbling blocks. But the challenge also lies in who's procuring and managing all of those apps internally.*

With the owners of SaaS apps spanning across multiple departments, security and IT professionals need to partner with app owners to ensure the SaaS environment is properly managed.

Solving the issues surrounding SaaS ownership requires understanding business goals, reasons, and pain points about why teams leverage the SaaS apps in the way they do.

And then there's the challenges and risks associated with how employees use SaaS apps.

*Let's look at some common situations.*





# Human Resources

HR teams use various SaaS tools to manage benefits and administration, learning and development, talent acquisition, employee engagement, and more.

## Related SaaS risks:

- *Processing plenty of sensitive business and employee data, such as Social Security numbers, employee addresses, and more through HR SaaS apps.*
- *Spearheading (often) the entire employee onboarding and offboarding process, where bottlenecks can easily happen. For example, HR may not have the bandwidth to keep up with new hires.*
- *Forgetting to notify other app owners to remove departing user accounts from other applications.*



# Finance

Finance teams may turn to all kinds of SaaS tools for managing contract work and invoices, expense management, working with vendors and financial institutions, and more.

## Related SaaS risks:

- *Finding that “sweet spot” with business data — combining productivity while being highly cautious in how sensitive data, such as company bank accounts and employee credit card data, is handled.*





# Sales and Marketing

SaaS tools used by sales and marketing help companies improve the way they target accounts, communicate to customers, and expand outreach.

## Related SaaS risks:

- *Having unparalleled access to sensitive customer data — a cornerstone in business — that can be shared extensively across multiple SaaS applications.*
- *Lacking full visibility into how the data is being used because of the integrations and interoperability of multiple SaaS apps.*

# R&D or Customer Support

Processes for teams in research and development or customer support may be entirely built on SaaS applications.

## Related SaaS risks:

- *Leveraging different types of SaaS apps that employees (unknowingly) may expose highly sensitive data, intellectual property, or even source code.*
- *Affecting the whole company's business performance and reputation if there are any disruptions to operations.*



There's a lot of complexity in these different scenarios. Yet, complications rise even more when employees look for other ways to boost their productivity. Employees may turn to seamless app-to-app integrations, or easy-to-use browser extensions and services, like Grammarly and Calendly. Though these integrations and extensions may help employees be more efficient, they inevitably add more sprawl to the SaaS stack.



*“Employees can start using SaaS applications without any involvement of IT and security teams. As a result, these teams are often unaware that the applications are being used and don’t know about the risks associated with them. For example, they might not know that sensitive data is now processed by a SaaS provider and cannot associate the appropriate security measures with the app. On their own, end-users often lack the expertise to configure the apps in a way consistent with the organization’s policies.”*

*In addition, modern SaaS applications rarely function as data siloes. They often integrate with other software. Such interdependencies and data flows are often not considered by the individuals who bring SaaS into the organizations. Late-stage discovery of such externalities can put unexpected burdens on IT and security teams and might prevent the SaaS application from achieving its full potential in a reasonable timeline.”*

— Lenny Zeltser, CISO, Axonius and faculty fellow at SANS Institute

# 4 Steps to Drive SaaS Collaboration

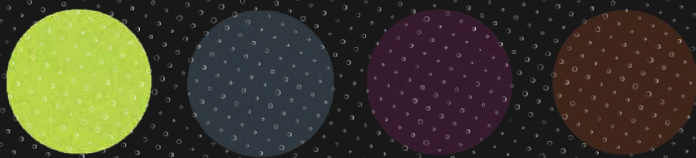
*Any SaaS management tool is only effective when there are collaborative processes in place.*



Internal stakeholders working with IT and security teams need to understand why a specific SaaS tool is necessary. It also means that SaaS app owners and admins are able to make configuration and management changes to reduce risk at the direction of IT and security teams. Without this collaboration, it becomes impossible for IT and security teams to keep up, maintain a strong security posture, and control SaaS spend.

*Here are four key ways to help everyone comprehend each other's needs.*

# Step 1



## Initiate SaaS adoption discussions.

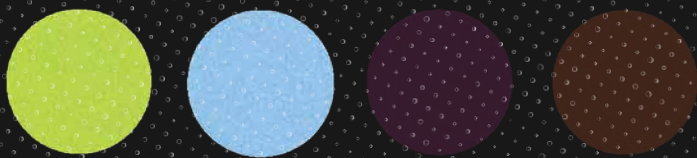
While you're understanding the use case for individual apps, you'll also want to take steps to learn about the broad SaaS usage across the company. Whether it's a survey, roundtable discussion, or another format, learn about the pros and cons of your company's actual SaaS environment today.

### **When it's time to work with stakeholders and SaaS administrators, IT and security teams need to ask essential questions, like:**

- *Which apps are essential to your teams?*
- *Which browser extensions are most commonly used by your teams?*
- *How are you managing user and data access to these apps?*
- *What service level agreements (SLAs) can you commit to, so you can address issues and misconfigurations that affect your company's security posture and finances?*



# Step 2



**Help your peers understand the big picture of all the SaaS apps across your company landscape.**

Build on what you learned from the stakeholders and acknowledge what effect the apps have on security and IT.

Yes, SaaS is highly user-centric. Each app offers a unique set of capabilities to increase employee productivity. Even with the benefits to employees, SaaS apps often gain access to extraneous company and user data, and integrate into internal IT systems and operations such as mail inboxes, calendars, and file storage.

In the end, the SaaS tool becomes part of the organization's attack surface that security and IT teams need to manage and protect.

*Be transparent and educate your peers about what's happening in your company's SaaS stack. Explain the implications of uncontrolled SaaS sprawl, and its impact on the entire organization.*



# Here's a look at the challenges of uncontrolled SaaS sprawl:

## The spread of shadow SaaS apps

- Employees use SaaS tools without the knowledge of IT and security, installing new apps or linking them to their personal accounts. Since many SaaS apps offer trials or purchase with credit cards, the rate of new SaaS apps being brought on has skyrocketed.
- Shadow SaaS expands the unknown attack surface by sidestepping security and procurement's typical vetting procedures. Many SaaS providers don't have the adequate expertise or measures in place to protect customer data.
- Employees may become targets — if not victims — of threat actors trying to gain access to the company's sensitive data. Shadow user accounts may expose that data by involuntarily providing access to internal file storage, business-critical apps, emails, calendars, and more.

## Non-compliance

Shadow SaaS makes your company vulnerable to non-compliance risks. HIPAA, GDPR, and other regulations define how companies can use, store, or transfer consumer data. Customers of SaaS apps (e.g., data controllers) may get hit with millions of dollars in fines even if SaaS providers are at fault for a security incident and don't have adequate measures in place.

## Spend optimization

The skyrocketing growth of SaaS adoption impacts spend. Various app owners are deploying SaaS apps with duplicate functionalities, and possibly overspending on app licenses, creating a lack of visibility into app utilization.

## Onboarding and offboarding gaps created by decentralized IT management

The more SaaS apps used by employees, the more the apps affect onboarding and offboarding. Specifically, most organizations have manual processes for onboarding and offboarding, meaning many user accounts are left active well after employees depart.

**These manual processes can create several issues, like:**

**1. Users onboarded with the wrong permission level**

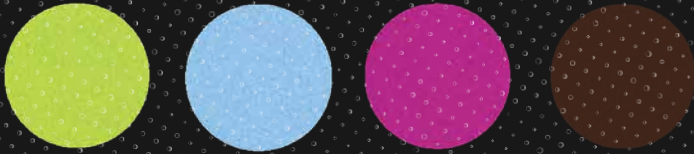
*New user accounts may be created with extraneous permissions, allowing users to view, export, and share sensitive data.*

**2. Offboarded employees with active SaaS user accounts**

*This is problematic since departed employees may still be able to access SaaS apps. It's also money being spent.*



# Step 3

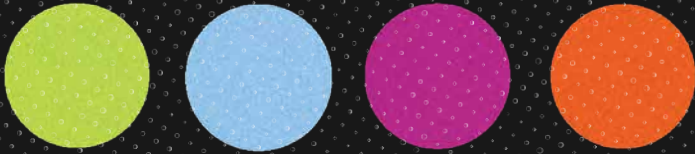


## **Establish, review, and enforce company policies around SaaS applications.**

- *Set standards, review SLAs, and develop a foundation for how employees use SaaS. For example, they must access these apps through single sign-on unless the SaaS apps don't support it.*
- *Develop thresholds around user privileges, like each app has a limited number of admin users required for the business.*
- *Ensure the established standards help adhere to and report on compliance to specific frameworks and certifications that are critical for your business.*
- *Establish a clear vetting process for onboarding new SaaS applications. Ensure these steps — risk assessment of those applications' frameworks and certifications adherence, security features, data handling, and potential exposure implications — are all done before the SaaS app is connected to your company's environment. Make the process of procuring new apps transparent with the data obtained being available to all internal stakeholders.*

***To start the conversation about your company policies for SaaS apps, think about having a messaging channel or ticketing system that includes all business stakeholders to escalate SaaS issues as they come about.***

# Step 4



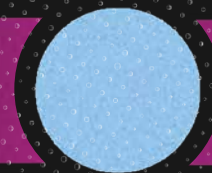
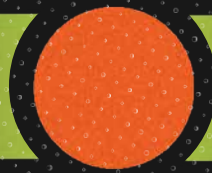
**Build a transparent, collaborative review process to continuously evaluate the effectiveness of your SaaS strategy.**

**The recurring SaaS app stack reviews (performed on at least an annual basis) should primarily focus around the following key areas:**

- *Continuous ability to discover “unknown unknowns”: shadow applications and users being added to the environment.*
- *Obtaining utilization insights for your most critical SaaS apps. A good place to start would always be the SaaS apps commonly employed by finance, sales, marketing, human resources, and research and development teams and handling your “crown jewels”: customer and business sensitive data. Not only should you review the handling of the data by and between those applications, but also evaluate if you have only authorized users and devices accessing the SaaS apps.*
- *Optimizing the settings and configurations of your SaaS applications, primarily around user permissions and session duration, multi-factor authentication, access to sensitive data for guest users, and more.*
- *Tracking your SaaS spending trends, app licensing versus actual utilization data, and any potential applications with duplicative functionalities in use across your company.*

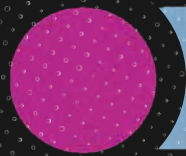


# A Comprehensive Way to Solve Pervasive SaaS Challenges



*It's clear SaaS has tremendous value to companies and employees.*

*An effective, company-wide SaaS strategy is imperative to protecting the attack surface. It's critical to work internally on streamlining the day-to-day SaaS operations.*



Different technologies now have emerged to help tackle these challenges, but many operate in limited ways. Take SaaS Management Platforms (SMPs), for example. SMPs help IT manage daily SaaS operations, track application usage, improve the employee onboarding and offboarding experience, and provide some visibility into SaaS licenses.

Although some SMPs have basic security functionality built in, they often lack robust details about SaaS settings, data flows, misconfigurations, and user access levels — information that's critical to reduce security risks.

There's an alternative that both reins in the complexity of the SaaS environment and protects the sensitive data stored in and shared between multiple apps.





**A comprehensive SaaS management solution should address three main areas to solve existing SaaS challenges and deliver business value to all stakeholders:**

1. **Breadth:** Detecting both known and unknown SaaS applications, with complete and actionable visibility into shadow usage, existing app onboarding gaps, and more.
2. **Depth:** Uncovering and mitigating various security risks (like user access policies, misconfigured SaaS settings, password procedures, and more) that put sensitive customer and business data at risk.
3. **Context:** Offering correlation and valuable data insights between the SaaS app environment, cloud services, devices, and users, to help control complexity across the company's IT environment.

**Tools like Axonius SaaS Management can both tackle the security risk and operational challenges of SaaS by:**

- Discovering all SaaS applications, including sanctioned, unsanctioned, shadow and unmanaged apps
- Gaining actionable visibility into interconnectivity flows between SaaS apps and third/fourth-party app extensions
- Uncovering and mitigating various security risks, like identifying suspicious or malicious behavior
- Obtaining insights on user access and app utilization for better IT management and cost optimization across all SaaS apps

**With a modern, comprehensive approach to SaaS management, IT and security teams have the confidence to effectively control complexity across the entire SaaS application stack.**





# See how you can gain control and manage the sprawl of SaaS apps, identify misconfigurations, and mitigate data security risks for a single source of truth through Axonius SaaS Management.

**SEE IT FOR YOURSELF.**

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](https://axonius.com).*

