The Tell All Guide to Solving SaaS Security and Governance

SaaS apps are exploding in use, with good reason, bringing SaaS security to front of mind. In this ebook, we outline (beyond the obvious reasons) how and why SaaS security and governance is actually good for business.

> *“It's "game on” in the saas environment. I think the reason is because it really is accelerating companies' ability to do more, to go further faster. And as security practitioners and as a security executive myself, our job is to ensure folks can do that but do it in a way that manages the risk appropriately.“*

- Steve Pugh, CISO at ICE. SVCI member

How SaaS Is Taking Over

SaaS is great, there's no doubt about it. No matter your organization, everyone uses some form of SaaS app in their day-to-day work, whether this is through Zoom or Slack or even Google Workspace or Grammarly, SaaS is everywhere.

There's no getting away from it.

The way people and organizations work has evolved immensely in recent years. People work in the Cloud more often than not. You need to grammar check quickly? You need to transcribe a video? You need to take a screen recording? There's an app for that.

Gartner predicts SaaS will remain the largest public cloud market segment, a forecast that came before COVID-19 changed the world of work and only exacerbated SaaS growth. Small- to medium-sized businesses (SMBs) use at least 110 SaaS apps, boosting not only productivity, but also in many cases quality of work. This is great, but it does introduce a whole new potential attack surface.

With the way we work evolving, so too must our SaaS security. SaaS is taking over, and you need to be ready.

The Main Challenges of Securing SaaS

While these cloud-based applications offer increased efficiency and productivity to an organization, there are significant threats placing organizations at risk for data leaks. Security leaders face these threats everyday. Unfortunately, in the rush to maintain productivity and introduce new SaaS applications, security is often overlooked by vendors, users and organizations.

In the first half of 2022 alone, there have been many examples of how SaaS apps are a target for malicious activities: In January, threat actors claimed they gained access to Okta's Slack channels which, according to the attackers, held massive amounts of sensitive data. In March, both Hubspot and Mailchimp were targeted and in April it was GitHub with stolen 3rd party app tokens. These are just a few examples.

SaaS Security Painpoints Include:

01 A Lack of Discovery and Analysis

Before you can address your SaaS security, you need to know and understand what you have and who is using what. Without a system in place in an organization to discover and analyze your SaaS estate, there is no way to identify if there is a specific application or multiple applications you should be concerned about. Without analysis there is also no way to prioritize which issues to deal with first.
You need to be able to rank your apps in terms of how secure they are and the implications for your organization if they don't hit the mark. This can be because the SaaS app doesn't have the correct compliances, or because it is too small an organization etc. And if you are not aware of the potential threats to the organization from SaaS applications, you are more likely to miss something.

02 Risky App2App Data Sharing

This lack of awareness extends to App2App connections . Apps regularly share data and many users do not even realize this level of sharing is occurring, exposing sensitive data. Users are unwittingly unaware that they are putting the organization at risk whilst simply trying to get their jobs done.

03 Open Ended External Data Sharing

Many users share data externally at the click of a button, think of a Google doc or a repository shared with a client, or to a third party provider. This can be risky, as often this data is shared indefinitely, even once users from either party have left the organization.

04 Problematic Permissions

When SaaS apps are tracked on an Excel without further analysis, organizations may miss inconsistencies or irregularities in the permissions apps are granted. Often it is quicker to grant blind permissions to save time or to increase productivity, but this may leave undetected security holes. For example, it's often easier to login to a new app with your Gmail instead of entering your name, organization and email etc., but this can unintentionally grant the app too many unnecessary permissions.

05

New App Onboarding Going Under The Radar

As more employees and divisions within an organization adopt SaaS apps, they can experience SaaS sprawl, which impacts their ability to have true visibility into what apps are being used – and who is using them. Many users work around IT policy and onboard apps on their own. Without oversight, users can use whichever applications they want and put the organization at considerable risk.

SaaS is dynamic and always on so in an attempt to add visibility, apps are often onboarded but not added in real time to the organization's database of SaaS apps in use. And manual tracking using a spreadsheet is not a tenable solution as it leaves multiple security holes in place often missing a large swathe of apps being used.

Lack Of Effective Remediation

Effective remediation is something that is easy in theory but difficult to implement effectively if you do not have the right resources and implementing it manually.

In a sea of inconsistencies, security gaps and orphan accounts, how can your organization combat the SaaS security risks that these pose?

There are three main ways that ineffective remediation can take place:

01

Not Utilizing The Correct Tools

Sometimes when an organization is aware of a breach or vulnerability within the apps, they often do not have the tools necessary to remediate or fix the problem. In some cases, users have too much work and forget to apply fixes. This can lead to vulnerabilities or breaches in the organization that could be easily avoided.

02

Partial Remediation

This is when you remediate only part of an issue. This can happen as sometimes you might not even be aware of the entire issue at hand. This is common for organizations that use security solutions that only monitor specific elements of your SaaS security. This can be problematic as it could lead to unsecured apps and potential breaches.

03

Delayed Remediation

Even with a good remediation plan in place, implementation can be problematic due to resources and time constraints. This means remediation is not immediate and is often delayed. An organization's security leaders can only do so much manually. In the cases that they are using software solutions for their SaaS security, usually they must check several different dashboards to get real time alerts, which is a strain on time and resources.

Remediation as a whole is ineffective unless it is scalable for your organization and automatic. Enabling automatic remediation skips all of these steps and enables security leaders to be much more effective in their roles. Remediation without automation can be as problematic as visibility without analysis.

Holistic Solution Versus Multiple Apps

As SaaS continues to increase in popularity and it becomes ingrained in our daily lives, many organizations have started to try to get a hold of their SaaS security. They do this by blacklisting apps, manually tracking new app onboarding and legacy CASB solutions. Theoretically, with your long list of vulnerabilities, you could enlist the services of 5 different vendors. These tactics are not sufficient and lead to gaping holes in your overall security.

An end to end holistic SaaS security solution that is always on saves your organization and security leaders a lot of time. You should be able to choose to engage and involve your end users and help them to be accountable to their SaaS security, if you wish. After all, they're the ones who know why they've given a specific app permissions. You, as the security leader, should be able to set up a remediation workflow that can automatically shut down risky App2App connections or enable you to have enough information to ask the user themselves why they have granted these permissions. Having everything together in one easy to use dashboard makes maintaining a high level of security a breeze, at the click of a button. This enables your security leaders to encourage and develop an overall strong security culture throughout the organization.

Shoring Up Defenses: SaaS Security and Governance Are a Necessity

We hope we haven't scared you away with all the risks, as here comes the good part, **the solution.**

A SaaS security solution that envelopes a holistic risk mitigation program is essential for effective security. Organizations need to seek out a SaaS security and governance solution that offers the following features for true coverage.

01

Assessing Your SaaS Estate With Non Intrusive Discovery and Effective Analysis

Before you can implement effective SaaS security, you need visibility into all of the SaaS applications that are being used in your organization, both active and dormant. You need this discovery before you can start to think about how to solve potential vulnerabilities and issues.

This discovery can help you to understand what SaaS apps are linked to the organization, what permissions these apps have and how long ago these were provided. Are these permissions still relevant to the user or the organization?
To gain a deeper understanding of your SaaS estate, implementing a security score across the board can help you to quickly see which apps need attention. This level of transparency should also allow you to see the compliance level of in-use and dormant applications, how big the organization that made the app is and where the app is based (country etc.) to name a few.

Ensuring the solution you use is non-intrusive to users and to the organization's data means privacy isn't invaded. A good SaaS solution will shy away from processing personal data, will use volatile and minimal permissions and will view user privacy as a top priority. It should be an example of how a SaaS app should behave.

02

Automated Remediation

Doing a thorough discovery and analysis of your SaaS estate is just the first step. At this point you should be aware of any and all security risks and vulnerabilities in your organization. You now need to be able to quickly and efficiently solve these issues. For example, if a vulnerability or suspected breach occurs, we can't always count on users to apply patches and updates (they are just a small part of fixing the issue). Turning a blind eye to issues is common – especially among busy users who lack time and resources. That's where automatic remediation comes in. Automatic remediation ensures reminders are not ignored because fixes are automatic after a certain specified period of time with customizable remediation paths. In addition, this automatic remediation should be able to disable or uninstall low security scored apps if the warning email was ignored by the user.

03

Engaged End Users

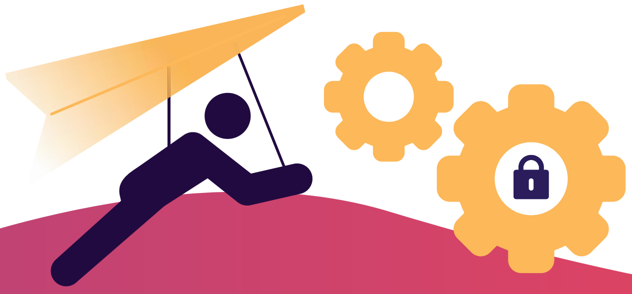
There is a lot going on with multiple SaaS applications in an environment that IT and security leaders may miss. Users are often unaware of problems or vulnerabilities that the apps they're using are exposing them to. The solution should enable users to own their security, and empower them to take action in the security process, if you choose. Get users interested, involved, and engaged in understanding security risks. Encourage them to protect corporate data with the same vigilance that they would use to protect their own personal belongings by involving them in the remediation process. Alerting users of risky apps, unnecessary permission they gave or problematic usage patterns while also explaining the rationale behind the alert - really goes a long way in ensuring users are security conscious and cooperating. Of course, your SaaS security solution should also give you the option to blacklist everything, if you want. The freedom to choose what works best for your organization is what sets security solutions apart.

04

Ongoing SaaS Analysis

Your security leaders are constantly spinning many plates, all at the same time. Unfortunately this means that sometimes, things can fall through the cracks. Whether it is risky App2App connections that should have been flagged or orphan accounts from previous employees, your security leaders can only do so much.

An end-to-end holistic, always on security solution saves resources, ensures human error is minimal and saves security leaders the hassle of integrating several solutions together. From discovery to remediation, everything needs to be covered on an ongoing basis. This way you can ensure that nothing is missed.



Your SaaS Security Checklist: **What You Need To Be Secure**

Solving the SaaS security issue goes beyond just tools and solutions. There are also several critical must-haves that you need in your organization to ensure you are addressing SaaS security.

Use this security checklist to start tackling your SaaS security today.

□ **Know your organization's complete SaaS estate**
Understand what apps your organization uses and are they worthwhile having? Seek to keep information such as app compliance, app maturity, app location, and whether or not the app uses encryption in one place.

□ **Get a security ranking for these apps in your SaaS estate**
Do any of these apps put your organization at risk?
If yes, why?

□ **Assess the App2App connections of your SaaS estate**
Are any of these App2App connections putting your organization at risk?

□ **Understand user behaviors**
External users with high permissions or users who use unwanted authentication methods are some examples of the information you need to have if you're going to keep a clean and secure SaaS environment.

□ **Understand and be in control of external file and repositories sharing**
What files and repositories are being shared externally?

□ **Engage your end users**
Engage users as part of the process of knowing what apps they are using and the risks associated with these apps.

□ **Always monitor when new applications are added**
Ensure a system is in place that no app is added without your security solution being aware of it.

□ **Build a Process**
Ensure proper protections are in place for when things go wrong.

□ **Build for Scalability**
As your organization grows, your solution will need to grow too. Ensure that no matter how many applications are in use and no matter how many users are in the organization, no application or permission is missed.

□ **Reporting based on data driven decisions**
Another important aspect to SaaS security is to ensure decisions are based on actual data. Having a solution that clearly displays what the situation is and prioritizes the actions is key so that you can make informed decisions.

Building a Secure SaaS Environment with Wing Security

01

Ensuring effective SaaS security doesn't have to be difficult. Your SaaS security solution should give you as much or as little control as you want. Do you want to blacklist all unapproved apps? You got it. Do you want to engage your end users to take part in the security process by prompting (or nudging) them to close unused apps or rectify potential problems easily? **You got it.**

02

Wing's SaaS security offers you the visibility to see into your actual account use. It offers automatic remediation, which is a great relief, as sometimes these prompts are missed when fixes are left in the hands of busy users or security leaders. It gives your organization a holistic approach to SaaS security, allowing security leaders to have one solution to flag, rank **and fix their security issues.**

03

With millions of apps available and we do love SaaS products– and their numbers growing daily - it makes sense to have SaaS security that you can count on to protect your users and the productivity tools they use.

Wing is easy to onboard and fully customizable to your organization's needs. Does it sound too good to be true? Let us prove it to you.

WING

Learn more by visiting our website

Wing Security

See it in action

Book a Demo