

CREATING AN EFFECTIVE SAAS SECURITY STRATEGY



SaaS applications are everywhere — used in every department and every industry. For many organizations, their SaaS stack often includes hundreds of applications. And SaaS can get very expensive, very quickly. In fact, some Axonius customers report **SaaS costs account for 50% – 70% of their total IT budget.**

After conversations with hundreds of IT and security leaders, we've assembled the following guide to form a comprehensive SaaS application security strategy.

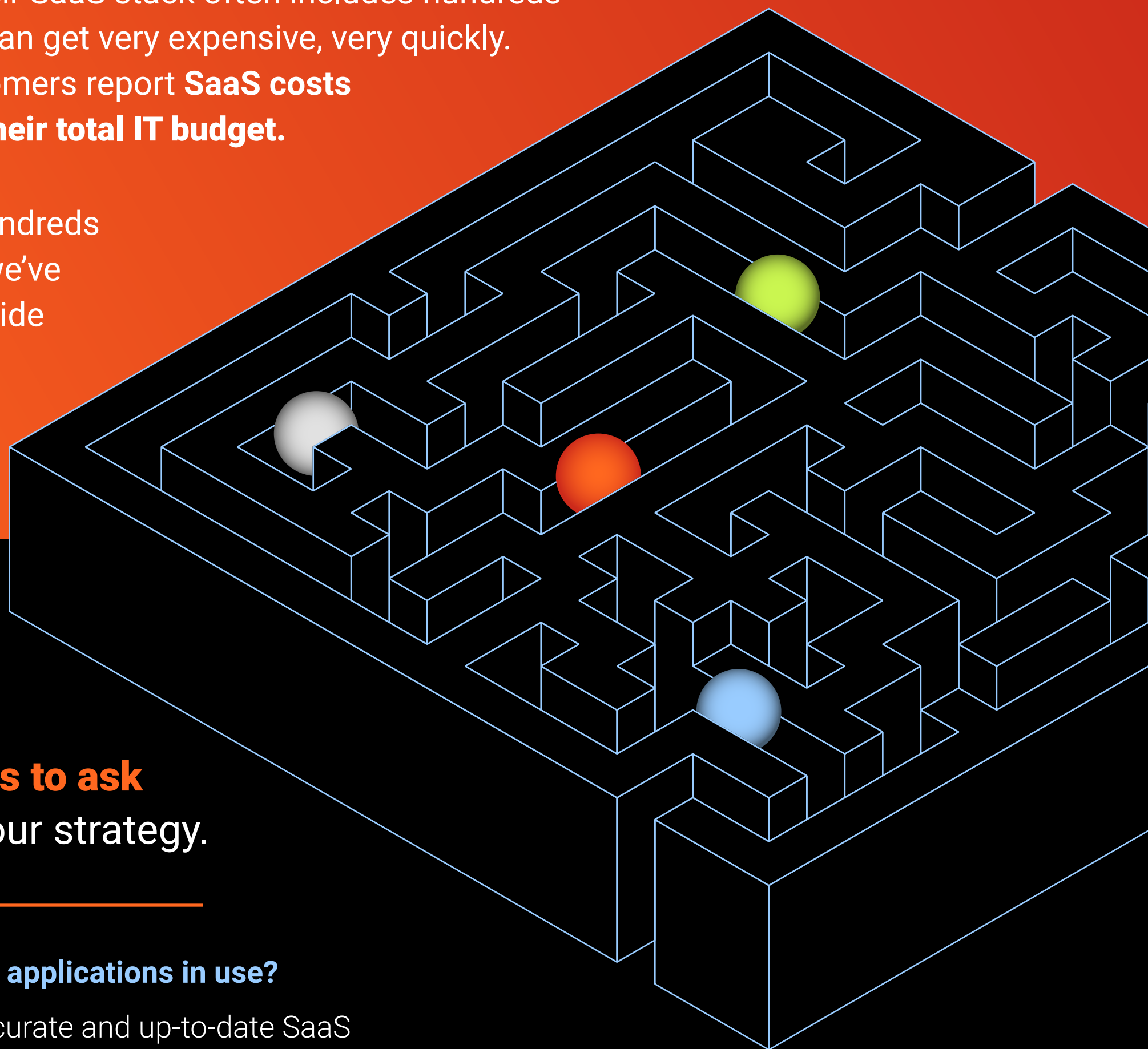
Read on to see **the most critical questions to ask and answer** to build your strategy.

How will we discover all SaaS applications in use?

Having and maintaining an accurate and up-to-date SaaS application inventory is a critical component of an effective strategy. With a comprehensive list of all SaaS apps, you can better understand overall SaaS usage, identify potential security and compliance risks, and optimize spend.

An effective SaaS app inventory includes details, like:

- > The number of users who have access to each app.
- > Information about the app's data security and compliance features, such as data encryption, user authentication, and regulatory compliance certifications.
- > The type of vendor subscription plan — monthly, annual, or per user.



What happens when an unapproved SaaS app is discovered?

Finding redundant or shadow SaaS apps can elevate security risks, add complexity to SaaS management, and negatively impact your security posture. All told, unsanctioned or unmanaged apps make it harder to ensure compliance, security, and governance. By leveraging a dedicated SaaS management solution, you can discover all SaaS applications – whether sanctioned, unsanctioned, shadow, or unmanaged. Once you have this information, you can take appropriate actions like removing and blocking the SaaS app in question.

What are the roles and responsibilities for procuring, configuring, and securing SaaS apps?

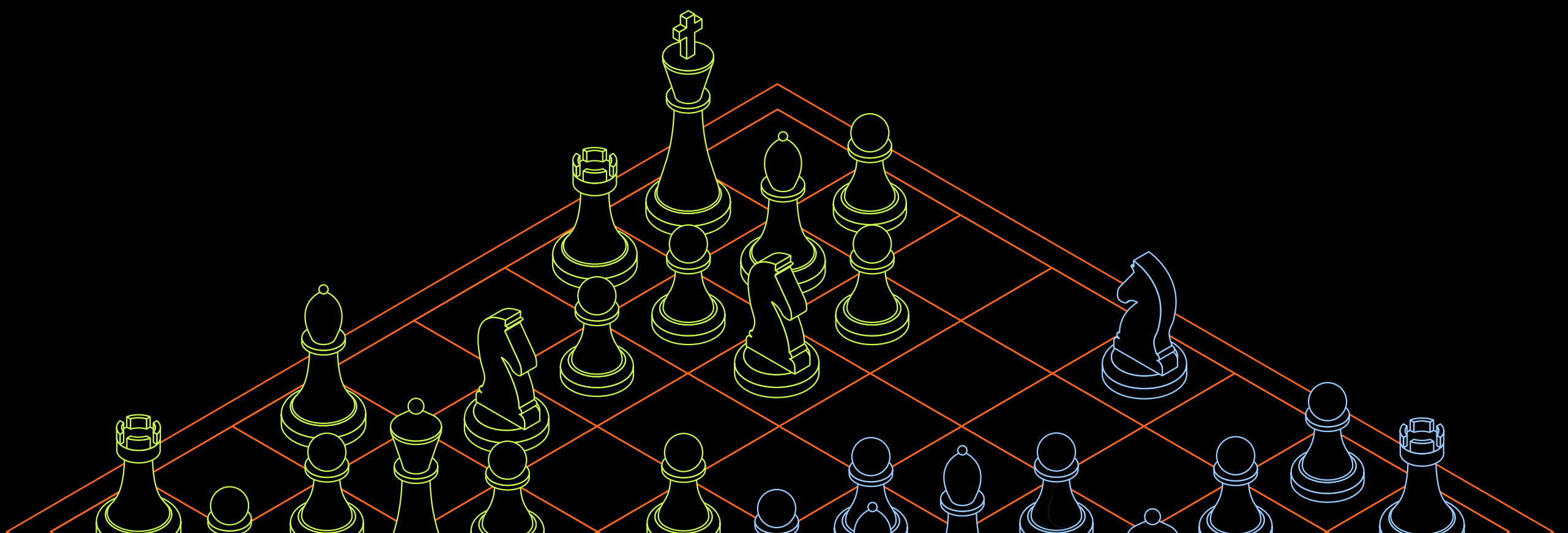
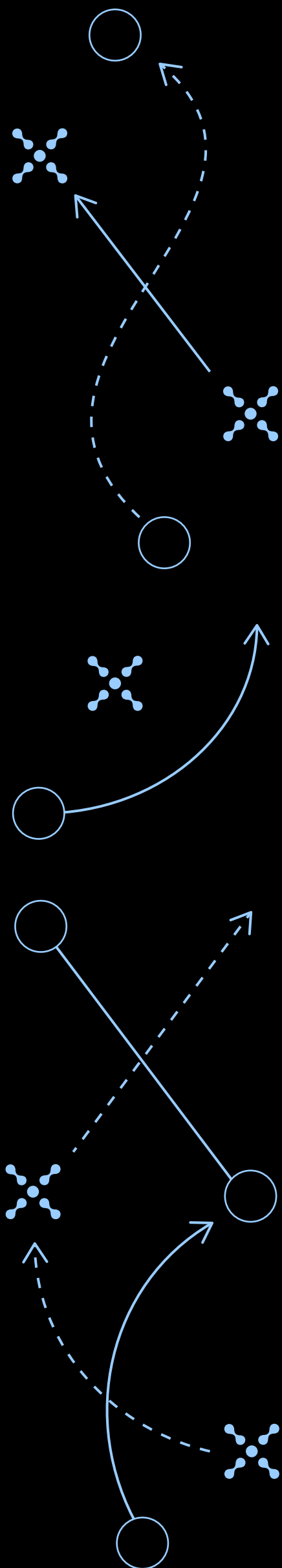
Collaboration is key to putting together a SaaS security strategy. IT and security teams must work with internal stakeholders (like finance, sales, and marketing) to understand why a specific SaaS tool is necessary. That also means SaaS app owners and admins making configuration and management changes to reduce risk at the direction of IT and security. Doing so helps maintain a strong security posture and control SaaS spend.


How will sensitive data be handled by SaaS applications?

Create a transparent, collaborative review process to continuously evaluate the effectiveness of your SaaS strategy. **Look at your most critical SaaS apps and their “crown jewels” – customer and business sensitive data.** Not only 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.

How will we monitor security issues, like misconfigurations, neglected and orphaned user accounts, and unusual usage and access?

With a dedicated SaaS management solution, you can continuously reduce the SaaS app attack surface by ensuring complete visibility into the SaaS environment. By doing so, you can correct settings configurations, conduct ongoing vulnerability and compliance checks across the entire SaaS app stack, and monitor for suspicious activity.





What processes will be in place for onboarding and offboarding employees?

Onboarding and offboarding are often done manually, potentially creating a whole bunch of security risks — and incidents.

Actionable visibility is key here. By understanding what's going on in the entire SaaS app stack, you can know where redundant apps, or underused or duplicate SaaS licenses are. Beyond spend, actionable visibility provides insight into SaaS security risks like shadow SaaS and weak access controls.

How will we ensure the SaaS applications we're using meet regulatory, policy, and compliance requirements?

Set standards, review service level agreements, and **develop a foundation for how employees use SaaS.** (For example, they can only 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. And ensure the established standards help adhere to and report on compliance to specific frameworks and certifications that are critical to your business.

How will we track and analyze SaaS spend?

Maintaining an accurate SaaS application inventory is important for effective SaaS cost optimization. Actions like identifying and consolidating redundant SaaS apps, and managing user access, roles, and permissions for SaaS licenses go a long way to control spend.

By focusing on key elements like **ownership, onboarding and offboarding, configuration, and monitoring**, you can put together a comprehensive SaaS security strategy. And have the **confidence to efficiently control complexity** across your entire SaaS app stack.

To learn more about putting together your own SaaS security strategy, request a demo today.

[REQUEST A DEMO](#)

