DoControl.

The CISO's Guide to SaaS Security

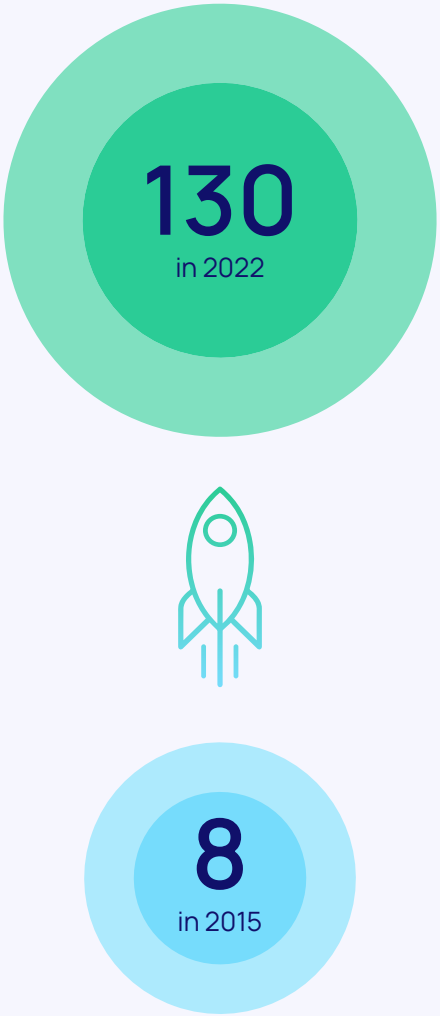
4 Key Approaches & Practical Tips



The prevalence of SaaS applications has skyrocketed in the past decade. The average organization currently uses 130 different SaaS apps, up from only eight apps in 2015. Unfortunately, the popularity of SaaS applications isn't restricted to the organizations who appreciate how they facilitate employee productivity. They are also an increasingly tempting target for cyber attackers. Bad actors are drawn by the growing bulk of sensitive data held in SaaS systems, SaaS' decentralized structure, and its interconnectedness with external SaaS applications. In a 2023 survey of over 3000 IT professionals on cloud security, SaaS applications were voted the top target for attackers.

This makes SaaS security a topic that is on the minds of most organizations. It's certainly on the minds of regulators, such as the United States Cybersecurity and Infrastructure Security Agency (CISA). In the past two years, CISA has issued and updated its Cloud Security Technical Reference Architecture to guide government agencies' adoption of cloud technology and piloted the Secure Cloud Business Applications (SCuBA) project to help secure agencies' cloud business application environments (like Microsoft 365 and Google Workspace) and protect information created, accessed, shared and stored in those environments.

Average number of SaaS applications used by organizations worldwide



To help you navigate through the maze of SaaS security and figure out what would best fit your organization's needs, we've put together this guide explaining:

4 aspects of SaaS applications that need to be secured
SaaS security approaches and what each will (and won't) protect

DoControl.

Four Aspects of SaaS That Need to Be Secured

Committing to securing your SaaS is fantastic, but it's about as actionable as making a resolution to "be healthier." Does "being healthier" mean you're going to address your eating habits? Cardiovascular health? Emotional wellbeing?

While SaaS is nowhere near as multifaceted as the human body and psyche, its multiple facets do need to be identified in order to appropriately address and secure each one. Let's take a look at the four main aspects of SaaS that need to be accounted for when it comes to security issues.

Data

When we think about securing SaaS, what often springs to mind first is the data contained within the SaaS ecosystem. To take an example from the physical world: a high-security bank vault is intended to protect the contents of the vault.

Protecting your sensitive, valuable data from exposure is critical for:

- Industry success (i.e. protecting trade secrets and maintaining competitive advantage)
- Regulatory compliance (i.e. avoiding the financial, legal and reputational consequences of a compliance breach)

Securing SaaS data involves:

- Discovering all datasets in the ecosystem
- Identifying which data is sensitive, personal or private
- Ensuring that data is only shared with, moved to, or accessed by relevant entities

Identity

No one keeps valuables in a vault if they never intend to use them. At some point they will be taken out and used - but it's critical that they be accessed and used by the right parties.

When it comes to SaaS, parties who may be accessing your data include employees and admins, as well as third-party collaborators and contractors. Securing the identity aspect of SaaS is making sure that the parties accessing and using your data are supposed to be accessing it - and that they are who they say they are.

Securing SaaS identities involves:

- Implementing strong authentication methods to verify user identities
- Reviewing and updating user permissions and entitlements
- Monitoring for unusual access patterns
- End-user education on security best practices

Four Aspects of SaaS That Need to Be Secured (Continued)

Third-party OAuth apps

It's not only human parties who have access to your data. Third-party OAuth apps are frequently connected with SaaS applications to streamline workflows and enhance productivity. And OAuth is secure… right?

OAuth, like anything else, has weaknesses that can be leveraged by bad actors. In the same way that you need to be on top of your human users, SaaS security necessitates keeping a close watch on your OAuth apps to ensure they are accessing only the data you want them to, when you want them to.

Securing SaaS third-party apps involves:

- Discovery of all connected third-party apps
- Rigorously vetting apps for security compliance and data privacy standards
- Implementing strict access controls, ensuring only necessary permissions are granted
- Regularly auditing and reviewing connected apps
- Promptly revoking access to suspicious or unnecessary third-party apps
- Prompt remediation of OAuth tokens if security breaches or vulnerabilities are detected

Configurations

What is the default security setup for your bank vault? What level of security clearance do you need to get near it? How much of the contents can you take out at once? These overarching rules are the first line of defense against any security mishaps.

The same is true of your SaaS solution configurations. These high-level application settings - like user access controls, data handling rules, network settings and security protocols - determine how the application operates. Ensuring that your configurations are secure is the foundation of protection against unauthorized access and data breaches.

Securing SaaS configurations involves:

- Compliance checks to ensure configurations meet relevant industry standards and regulations
- Visualization and remediation of misconfigurations
- Continuous monitoring and alerting of configuration changes

Four SaaS Security Approaches (and What They Protect)

Complete, holistic SaaS security must address all aspects: data, identity, third-party apps and configurations. Leave one out, and you have a gaping hole where your SaaS health can be threatened.

Do the SaaS security solutions out on the market today address the above aspects of SaaS security? Which aspects does each type of solution cover? We're about to dive in and get some details, but one word beforehand:

We only deal here with API-based solutions, and not agent-based solutions.
Here's the difference, and here's why:

Agent-based SaaS security solutions work by deploying software agents on user devices to monitor and control access to cloud services. All traffic must pass through the agent on its way from the device to the SaaS application or vice versa.

While agent-based solutions provide real-time user activity monitoring and security enforcement, that control comes with a deal-breaking tradeoff: information traffic jams. Traffic just cannot move at the same rate when it needs to pass through a tollbooth or security checkpoint. SaaS is built for speed and scale - of the user and of the developer deploying the SaaS. External, agent-based traffic controllers inherently cannot keep up the pace.

API-based SaaS security solutions integrate directly with cloud service providers via APIs to monitor and secure data. API-based solutions are non-intrusive, monitoring the data going back and forth between user device and cloud application without impeding the flow of information. These solutions are designed to develop and scale along with the SaaS application itself.

The API-based solution's one big drawback? Unlike the agent-based solution that checks all data flow before it crosses the boundary between user device and SaaS application, API calls can only note what happened after the fact. The lag is dependent on the API polling intervals and can range from seconds to hours (or more), but it is definitely not real-time, which delays the identification and remediation of security issues. The lag can be significantly reduced depending on the type of API-based solution chosen.

And now, for the SaaS approaches and which aspects of SaaS protection each of them cover:

SaaS Security Posture Management (SSPM)

SaaS Data Loss Prevention (DLP)

SaaS to SaaS Protection

API-based Cloud Access Security Broker (CASB)

SaaS Security Posture Management (SSPM)

COVERAGE: CONFIGURATIONS

SaaS Security Posture Management is an approach that continuously assesses and manages the security settings and configurations of SaaS applications, ensuring they comply with best practices and policies to prevent data breaches and unauthorized access. SSPM tools identify misconfigurations that could lead to data becoming publicly accessible, independent of specific user registration, creation or action.

In short, SaaS Security Posture Management is aptly named. It manages "posture" only: how your organization stands, but not how it moves. SSPM tools give a static picture that is helpful for what it does show. They do not address any dynamic aspects of SaaS use, however, and it is those that form the vast majority of SaaS security risks.

What SSPM helps with:

Discovering where your SaaS configurations may have left your organization wide open to risk.
An SSPM solution provides a bird's-eye view of your SaaS access controls or security settings and points out where improper configurations have left your ecosystem open to unauthorized access, data breaches or cyber attacks. This is the low-hanging fruit of SaaS security, so you don't want to miss it.

Eliminating barriers to compliance
Most organizations are subject to general or industry-specific data protection regulations, and non-compliance can result in serious legal and financial repercussions. SSPMs can check that no major overarching issue like a misconfiguration has left the organization exposed.

What SSPM does not help with:

Protecting the data and identity attack surfaces
The more users that are involved in a digital environment, the more **identity** becomes a possible attack surface. And the more data that is created and shared in that environment, the more **data** becomes a possible attack surface. SaaS is characterized by broad end-user ownership and access control over data. In SaaS environments like Microsoft 365/ Teams, Google Workspace or Slack, end users probably include everyone in the organization, and often people external to the organization, such as contractors, vendors and partners. That's a lot of hands in the pot. But SSPM only looks at high level configurations that direct data management, not at the data itself or how it is accessed, stored and shared by users.

Protecting against over permissioned or data-leaking third-party OAuth apps
If your SaaS has configurations that relate to third-party apps, an SSPM can highlight configurations that leave your organizations open to risk. But this third-party permissions management is all-or-nothing. SSPMs cannot distinguish between this OAuth app that you want to have read/write access to your database, and this other OAuth app that you only want to have read access. And, as with user-shared data, SSPMs cannot monitor the actual data being shared over or by the third-party apps.

Historical SaaS data exposure
Organizations can look at their SSPM to identify and fix misconfigurations going forward. But SSPMs do not provide a way to locate and fix data exposure that has already occurred due to misconfigurations. If an organization has been using a SaaS solution for any significant length of time, they are likely to have a large number of overexposed assets that the SSPM will not help them address.

In short, SaaS Security Posture Management is aptly named. It manages **"posture" only: how your organization stands, but not how it moves**. SSPM tools give a static picture that is helpful for what it does show. They do not address any dynamic aspects of SaaS use, however, and it is those that form the vast majority of SaaS security risks.

SaaS Data Loss Prevention (DLP)

COVERAGE: DATA

A SaaS Data Loss Prevention solution actively monitors data shared over the SaaS application for signs of leakage - whether through loss, theft or exposure. The DLP solution checks whether the content of the data and the way it is being shared violate predefined data security policies. If so, the solution can send alerts or take steps to remediate the situation.

What SaaS DLP helps with:

Preventing data exfiltration
A DLP solution can identify attempts to transfer sensitive information outside the organization, like sending files to personal email accounts, copying to external storage devices, or uploading to unsanctioned cloud services.

Preventing public sharing of sensitive data
A DLP solution can flag instances where sensitive data is mistakenly shared publicly, such as sharing social security numbers on Slack or credit card numbers in a publicly shared Google Drive document.

Monitoring data exchanges in third-party apps
Some SaaS DLP solutions can monitor the data being shared over or by third-party OAuth apps connected to your SaaS environment.

What SaaS DLP does not help with:

Controlling sharing of sensitive data with unauthorized parties (while still enabling sharing with authorized parties)
DLP tools identify data, not users. If the data is classified by your data security policies as sensitive, DLP will flag it when you try to share it. It doesn't matter if you're sharing it with a coworker in your department (which is okay) or with your third cousin (which is not okay). This inability to distinguish between appropriate and inappropriate sharing by users leads either to over-active alerting or overly permissive policies.

Protecting against over permissioned third-party OAuth apps
SaaS DLP solutions can often monitor the actual data being shared over or by the third-party apps. But they cannot evaluate the permissions given to those apps and come to conclusions as to whether the permissions should be reviewed or revoked.

In short, SaaS DLP solutions can address **content, but without context**. They do take into account the dynamic picture of changing and moving data, but the view is limited to **what** the data itself contains, **where** it came from and where it is going - but not **who** is involved in the data change or movement. Standalone DLP tools do not have the broader view of the user context and cannot incorporate that into their actions.

SaaS to SaaS Protection

COVERAGE: THIRD-PARTY OAUTH APPS

A Saas to Saas Protection solution monitors the non-human identities in your SaaS ecosystem, such as OAuth apps, service accounts, and applications that connect via webhooks, as well as the actions they initiate. It provides visibility into third-party apps and their access permissions, detects over-privileged or untrusted connections, and can alert to or remediate suspicious app activity.

What SaaS to SaaS Protection helps with:

Protecting against over permissioned third-party apps
SaaS to SaaS Protection solutions can evaluate the purpose the apps serve within your ecosystem and the current permissions given to those apps, then come to conclusions as to whether the permissions should be reviewed or revoked.

Protecting against untrusted or illegitimate third-party access
SaaS to SaaS Protection solutions are able to identify suspicious apps and app activity, often initiating automated workflows to remediate potential problems before they develop into actual security issues. They also take care of access token lifecycle management, reducing the risk surface created by untracked, exploitable tokens.

What SaaS to SaaS Protection does not help with:

Preventing data exfiltration, especially by insiders
A SaaS to SaaS Protection solution can see the identity and general activity of third-party applications, but it cannot see the actual data that is being sent. Therefore, it is not effective against insider threats that involve using trusted third-party connections and innocuous-looking activities to transfer sensitive information outside the organization.

Preventing public sharing of sensitive data
Similarly, since the SaaS to SaaS Protection solution does not read the actual data transferred, it cannot detect instances where sensitive data is mistakenly shared publicly, if such sharing happens through legitimate channels and connections, such as sharing social security numbers on Slack or credit card numbers in a publicly shared Google Drive document.

In short, Saas to Saas Protection solutions are an important component of securing the **non-human interactions** with your SaaS ecosystem and data, but their view is limited to **identity** and a very **zoomed-out picture of activity**. The details of that activity (i.e. exactly which data) and potential manipulation of legitimate third-party apps and connections by human actors is beyond their purview.

API-based Cloud Access Security Broker (CASB)

COVERAGE: DATA, IDENTITY, THIRD-PARTY OAUTH APPS

An API-based Cloud Access Security Broker (CASB) is a security policy enforcement solution for data moving through cloud applications. It uses APIs that integrate directly with the cloud service provider to monitor assets and user access. Upon finding a policy violation, a CASB initiates workflows to remediate the issue or alert security teams.

What CASB helps with:

Protecting against data exfiltration or exposure, taking user identity into account
CASB solutions include a DLP component, so they can monitor the content of every data asset in order to identify if sensitive data is overexposed. Unlike standalone DLP tools, however, CASBs can consider user authorizations (e.g. what level of permissions) and identity (e.g. within organization vs. external), making alerts and remediation workflows much more targeted and effective.

Monitoring user access and behavior
CASBs combine awareness of user authorizations and identity (often through integration with Identity and Access Management systems) with log analysis and behavior analytics to identify policy violations or anomalies relating to user activity.

Protecting against over permissioned or data-leaking third-party OAuth apps
CASB solutions can monitor the actual data being shared over or by the third-party apps with the DLP component of CASBs. They can also evaluate the permissions given to those apps and come to conclusions as to whether the permissions should be reviewed or revoked.

What CASB does not help with:

Discovering where your SaaS configurations may have left your organization open to risk
CASBs do not analyze or alert to SaaS misconfigurations or risky default configurations. Misconfigurations are actually a smaller risk factor in SaaS security than in other as-a-service solutions, such as Infrastructure as a Service (IaaS) or Platform as a Service (PaaS). According to the shared responsibility model for cloud security, the SaaS provider is responsible for platform- or infrastructure-level settings. Application-level configurations are handled by the SaaS customer admins, but a misconfiguration on that level will have a much smaller possible scope of effect and damage. The bigger and more exploitable attack surface in SaaS is the data, because the scope of data access is all users. Protecting the actual data, therefore, is a more critical issue for SaaS than protection against misconfigurations.

The bottom line on CASB

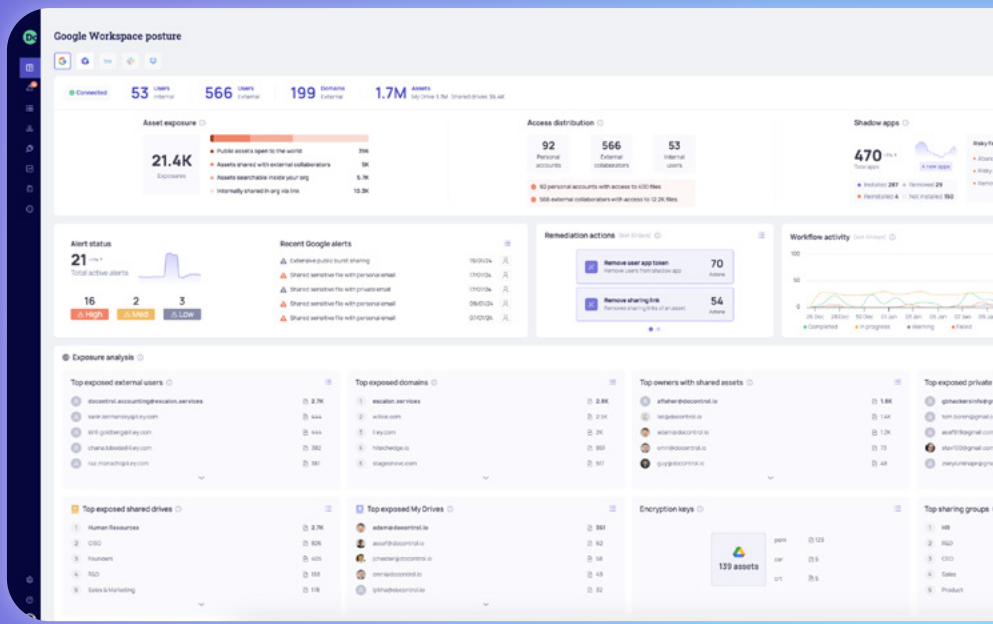
CASBs focus on the data itself and combine content and context, making them the most comprehensive SaaS security solution. There are differences even between API-based CASBs. Some use pull APIs, while others are designed to use push events. That technical difference has an impact on speed and performance. Some CASBs only take the context of the user into account, whereas others expand the user context to that of the business (e.g. what team is the user part of, what actions are typical of that team, etc.).

To effectively secure your SaaS environment in the light of ever-increasing applications and corresponding threats, take the time to identify the vulnerable aspects of your environment. Look at your data, configurations, and identities - both human and non-human. Then evaluate the SaaS security approaches and solutions, and see which best fits your organization's current needs, keeping in mind all the aspects you need to protect in order to be truly secure.

DoControl.

DoControl is a SaaS Security solution offering complete visibility, threat detection, and remediation for SaaS data exposure, insider threats, and over-permissioned third-party applications. Tailored for SaaS data scale and speed, the solution combines CASB and DLP capabilities to ensure protection across major SaaS ecosystems, including Google Drive, Slack, Microsoft SharePoint, Salesforce, and Box. Unlike traditional solutions, DoControl integrates business and security context for swift response to threats and effective insider risk management.

Protecting billions of SaaS assets, DoControl serves enterprise customers across multiple industries, including technology, media & entertainment, financial services, retail, and education. Headquartered in New York City, DoControl is funded by world-class investors, including Insight Partners, StageOne Ventures, Cardumen Capital, RTP Global and CrowdStrike's early stage investment fund, the CrowdStrike Falcon Fund.



Visit Our Website