Solution Brief

A Guide to SaaS Access Control and Management

SaaS access control determines which employees are authorized to use SaaS resources to perform daily tasks. It is a central component of SaaS security, as these services can expose companies to several risks if left unchecked. This guide provides an in-depth discussion of SaaS access controls to help CISOs, information security directors, and similar executives achieve more effective SaaS access management.

User Access Challenges for SaaS Security

Part of the reason access control for SaaS is so important is that SaaS services control and operate everything in the digital enterprise – from factories and finance, HR to IT – everything runs on SaaS. But given the nature of SaaS services, residing completely outside security control, managing users and access is difficult. Additionally, SaaS acquisition is decentralized, which means employees acquire it themselves. This differentiates SaaS from those the IT department procures, supervises, and secures. Since the purchase of SaaS can occur without security managers knowing, it is often referred to as shadow SaaS.

The complexity continues...not all employees use SaaS the same way. For example, one user may perform actions on a SaaS application that do not align with their position or access permissions. Furthermore, since the IT department seldom controls SaaS resources, the only means for managing protection is the identity.

These challenges indicate the need for a universal SaaS access control. Enabling secure access to SaaS services – easy login, strong authentication – and scalable, adaptive protection throughout the enterprise SaaS layer.

SaaS Verification and User Confirmation

Using SaaS is a part of modern work today, and users are accustomed to finding and using new SaaS apps as needed. With a robust access control strategy, you can implement a SaaS verification process that allows users to explain the need for a new SaaS app and implement access controls when security policies are violated.

Collecting this information can be done through an automated survey that is required, with the failure to do so resulting in blocked SaaS app access.

Without the enforcement mechanism, the survey response rates will be very low. Below are some examples of information that can be collected.

- Purpose of the SaaS app: Users should explain why they need the app and whether the functionality they are looking for is not available among the existing sanctioned apps they have access to.
- Data used by the app: Users should identify the type of data that will be used so security and compliance can understand what laws or company policies apply.
- User compliance: Users should acknowledge that they know and understand the company's data, privacy, and security policies and that using the new SaaS app does not violate any of those policies.
- User group: Users should explain who within the company will be using the app and whether external vendors will also have access to the app.

How to Control and Manage SaaS User Access

The main concern with SaaS is that the business has little to no control over it. If employees use personal devices to access these services, you may not have jurisdiction over the endpoint. In other words, you cannot conduct SaaS access management through cloud access security brokers (CASBs) or security service edge (SSE) – the process must be performed through identity. Identity solutions present their own set of challenges. Most identity products are designed for known SaaS apps, such as single sign-on (SSO). Additionally, many rely on voluntary methods like identity providers or password managers. These solutions have the right idea but can be costly to implement or not adopted by users. For example, password managers require users to enter their passwords into the tool, and most users resist doing so. In short, identity as a key point works in theory, but its implementation presents several flaws that cannot be ignored.
More recently, we see the rise of an architectural approach with the SaaS Security Control Plane (SSCP) which maps user-SaaS relationships and identity and SaaS risks based on accessibility and scope of SaaS control (SaaS facets and capabilities), followed by orchestration and enforcement directly or through integrations with existing enforcement points.

The Benefits of an SSCP for SaaS Access Control

Access control for SaaS is a multifaceted process that only encompasses a sliver of the complexity that these resources present for information security managers, architects, and analysts. For greater peace of mind with SaaS security, businesses may need a more comprehensive solution, such as a SaaS Security Control Plane (SSCP).

One of the most valuable capabilities of SSCP is its ability to look back through time to capture SaaS risks from 10+ years of user-SaaS relationships—from the first observed interaction to the present day. Consequently, companies can quickly remove a decade of risk with better awareness of SaaS services, users, groups, tenants, and policies taken from real-world usage. After initially removing accumulated risk in the enterprise SaaS layer, many organizations leverage the SSCP to identify security gaps in access control as well as user access reviews and authentication methods (IdP, OAuth, OIDC, passwords, etc.) across all SaaS services, users, groups, and tenants.

Finally, security teams reach a stage of SaaS security maturity by using existing controls—SSO, CASB, CSPM, CNAPP, SSE—to harness SSCP's insights, intelligence, and access control for SaaS today and adaptive to SaaS yet to be deployed.

With the SSCP, your organization can find, prioritize, secure and arrange security for all SaaS apps, whether sanctioned or unsanctioned. It also allows for secure access from managed and unmanaged devices, enabling your enterprise to pursue a safer business-led IT strategy.

Other benefits of the SSCP include:

- Discovers new SaaS apps that employees utilize
- Delivers enforceable access control (as opposed to voluntary access control)
- Covers SaaS that does not use identity products
- Handles SaaS impacted by employee offboarding
- Detects inconsistencies with SSO

Attain Better Access Control for SaaS with Grip

IT leaders that wish to achieve more effective SaaS access control at their businesses should turn to Grip for an innovative SSCP. This platform will enable your business to modernize its security framework and strengthen SaaS access. We lower the number of employees and resources needed to utilize our services while still delivering a fast time to install and a quick return on investment. Additionally, you can save money on SSO with the SSCP. To learn more about this service and SaaS access management in general, request a demo from Grip today.