Data Sheet

Grip SaaS Access Control

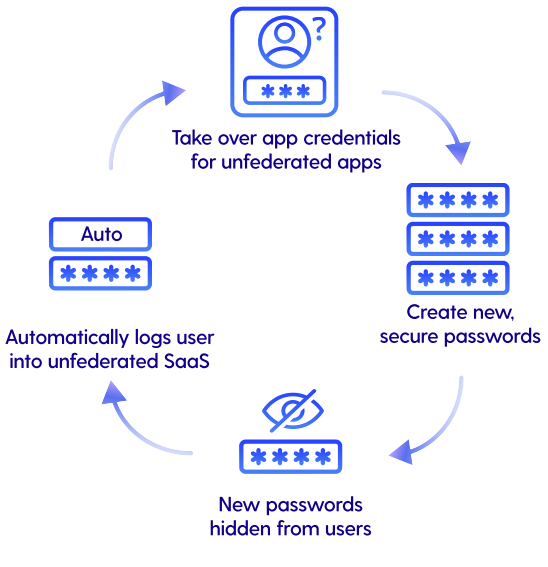
Control user authentication, authorization, and access management for unfederated apps or systems. SAML-less SSO governance for non-SSO apps or ones that do not support federated authentication.

SaaS Identity Risk Management

The surge in SaaS adoption has transformed the way people work, and modern cybersecurity needs to adapt to the reality that SaaS adoption will continue to increase. This is creating a need for comprehensive governance and control for not just core enterprise applications, but every application, and this has never been more apparent. Just as Single Sign-On (SSO) provides centralized control and monitoring of application access, shadow SaaS demands similar vigilant oversight to mitigate risks and prevent breaches.

SaaS Identity Risk Management (SIRM) has emerged as a cornerstone of modern cybersecurity, discovering, prioritizing, securing, and orchestrating security specifically for SaaS applications and cloud services. Traditional security control points, once effective, have faced erosion in the wake of SaaS's pervasive influence. The traditional combination of network, endpoint, and application controls falls short, underscoring the need for a new approach that focuses on the identity-centric risks that are pervasive today.

As organizations struggle to understand their SaaS identity risk landscape, the implementation of effective shadow SaaS governance becomes an imperative. SSO centralizes application access for the approved and sanctioned applications, but it is usually about 10% of the overall number of applications used in a company.



Grip SaaS Access Control

Key benefits & capabilities

Control Shadow SaaS Access
Improve security, compliance, and reduce the potential for security breaches by controlling employee usage of shadow SaaS.

Enforce Shadow SaaS Policies
Proactively enforce risk and compliance policies by automatically controlling business justification and controlling user access

SSO-like Monitoring for Unfederated SaaS Usage
Provide SSO-like monitoring and tracking of unfederated SaaS app usage such as logins, date/time of access--reclaim unused licenses

Lower SSO Costs with SAML-less Governance
Avoid upgrading to enterprise license tiers and incurring the enterprise security tax with SAML-less SSO governance

Securely Share Accounts
Share login credentials for apps while maintaining individual user activity tracking and maintaining credential hygiene processes such as password changes and sharing

Grip SaaS Access Control

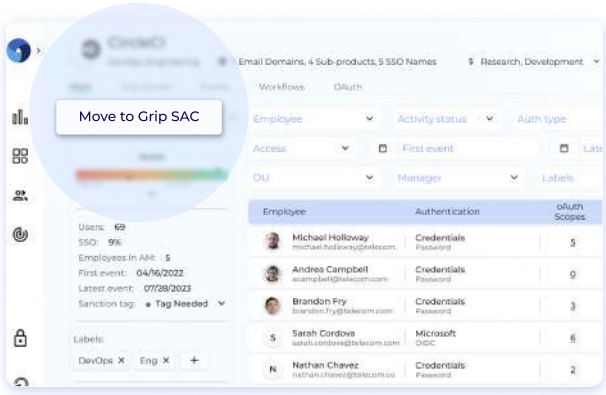
The Grip SaaS Access Control (SAC) product works with the Grip SaaS Security Control Plane (SSCP) to deliver SaaS identity risk management. It is deployed as a browser extension and provides more granular data on an employee's usage of unfederated SaaS applications. The award-winning Grip SSCP helps companies manage their SaaS identity risks by taking an identity-centric approach to discover, prioritize, secure, and orchestrate security workflows across a wide range of systems and applications. When used together with the Grip SSCP, the combination provides the industry's most comprehensive solution for visibility and security for unfederated applications.

Grip SAC leverages the Grip SSCP's discovery and robotic process automation capabilities to discover, secure, and control access to unfederated SaaS applications. It does this by taking over the credentials, creating new, secure password, and storing them in a secure vault that does not reveal the password to the user. The Grip SAC browser automatically logs the user in by opening a new browser window or entering their credentials when they navigate to the login page, similar to what password managers do. However, the key difference is that Grip SAC users do not know the password, and it is never revealed to them. This provides a higher level of protection control of unfederated SaaS identities that is like what is provided by SSO systems.

Take Over App Credentials For Unfederated Apps

Working with the Grip SSCP, security teams can take over a user's credentials for an unfederated SaaS application and store them in Grip SAC. The password is changed to one that meets the company's policies, and this new password is not revealed to the user. Users are automatically logged in for an SSO-like experience.

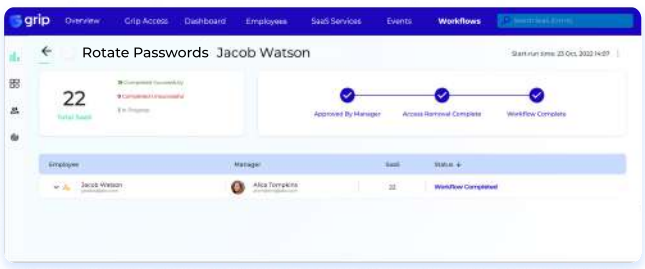
- Select the highest risk unfederated apps and move them to Grip SAC with a single click or automate the process for new users of the app
- Provide users with a seamless login experience where they do not have to remember passwords
- Avoid weak or reused passwords across multiple accounts and maintain strong password hygiene.



Move to Grip SAC

Create New, Secure Passwords

Working with the Grip SSCP, security teams can take over a user's credentials for an unfederated SaaS application and store them in Grip SAC. Through this process, the password is changed to one that meets the company's policies, and this new password is not revealed to the user. Users are automatically logged in for an SSO-like experience.

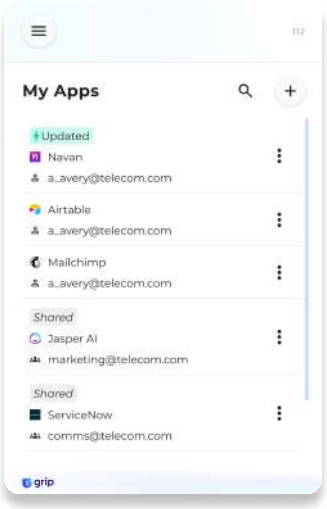


Automatically Rotate Passwords

Conceal Passwords From Users

Enable IT or security to select unfederated SaaS apps where the user does not have control of the password. Store passwords in a secure vault that is inaccessible by the user to be reused on unmanaged devices without the user authenticating themselves with the Grip SAC browser extension.

- Revoke user access with a click of a button for unfederated SaaS apps for workflows such as user or SaaS offboarding
- Eliminate the human factor for phishing attacks since the user does not know the password

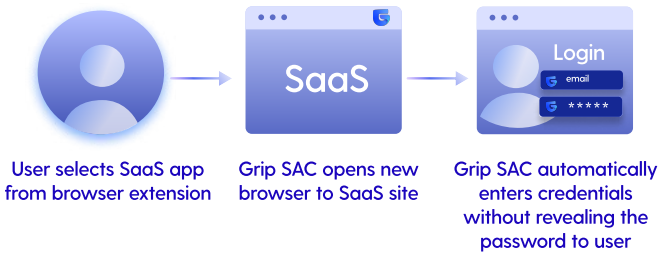


Conceal Passwords in Vault

Automatically Logs User Into Unfederated SaaS

The Grip SAC streamlines the user experience and enhances security by automatically logging users into SaaS applications or internal systems. Capture login activity and session details for audit and compliance reporting.

- SSO-like monitoring for login events for unfederated SaaS apps for audit and compliance
- Capture session details including session start and end times for unfederated SaaS apps



User selects SaaS app from browser extension

Grip SAC opens new browser to SaaS site

Grip SAC automatically enters credentials without revealing the password to user

SSO-like User Experience

Secure Credential Sharing

The Grip SAC enables teams to share login credentials securely with individual users or groups defined in an identity provider. A centrally defined access administrator controls who has access to the credentials. Users login using the Grip SAC browser extension and do not know the password itself. Each user's activity is monitored even though they are using the same login credentials. Password changes due to personnel or security workflows are automatically updated and all authorized users maintain seamless access without disruption.

- Share SaaS or internal system login credentials among users or groups and maintain logging and tracking of individual user activity
- Change passwords for personnel changes or offboarding without impacting user access
- Automate shared password hygiene by rotating it on a regular basis

Access admin creates shared credentials

Grip SAC creates password and conceals from the user

Share concealed credential with users or groups and log each person's activity

Share Passwords Securely

Data Sheet

Use Cases and Capabilities for Unfederated SaaS Applications

Use Case and Feature	Description
SAML-less SSO Governance	
SAML-less SSO	Govern unfederated SaaS apps without upgrading to enterprise license tiers
Centralized login monitoring	Detailed reporting of login events similar to what is provided for SaaS governed by SSO products
Revoke SaaS access	Turn off user access by removing the credentials from the user's Grip SAC vault
Save licensing costs	Reclaim unused licenses to reduce subscription costs
Enforced Password Hygiene	
Automatic password rotation	Periodically change passwords through automated workflows
Enforce strong passwords	Require passwords to be unique and meet corporate standards
Secure Credential Sharing	
Share logins among users	Securely share logins without revealing the password to individual users
Share logins among groups	Securely share logins without revealing the password to groups defined in the identity provider
Track usage of shared credentials	Log and report on individual user activity using the shared credentials

Data Sheet

Use Cases and Capabilities for Unfederated SaaS Applications

Use Case and Feature	Description
Auditing and Logging	
Track login events	Maintain detailed login tracking for auditing or compliance reporting
Monitor sign in events for all apps	Log and report all sign in activity regardless
Phishing Proof Passwords	
User inaccessible passwords	Prevent phishing attacks by moving passwords to Grip SAC and not revealing them to users
Automatic password rotation	Reset passwords automatically to protect against potentially compromised credentials
One click password reset	Reset passwords for all users for unfederated applications when a SaaS credential breach occurs
MFA Everywhere	
Require MFA for unfederated SaaS	Implement multilayered access and strengthen identity security by requiring MFA for unfederated SaaS apps