



The Grip-SailPoint Joint Solution

# Extending Identity Governance to Shadow SaaS

## The Challenge

Enterprises rely on identity security solutions like SailPoint to efficiently manage user access to applications. SailPoint simplifies and automates key identity processes—such as access certifications, provisioning, deprovisioning, and access requests—driving organization-wide efficiency.

While SailPoint excels at governing known, managed applications, the rapid adoption of shadow SaaS—applications procured and used without IT oversight—has introduced new challenges. These unmanaged apps create gaps in visibility and governance, increasing risks for organizations.

Through its partnership with Grip Security, SailPoint addresses this growing need by extending its capabilities to discover and manage tens of thousands of previously unknown shadow SaaS apps. Together, they deliver a comprehensive solution for full SaaS visibility, governance, and control, empowering enterprises to stay secure and compliant in an evolving SaaS landscape.

## The Solution

Grip Security, the pioneer in SaaS Identity Risk Management, and SailPoint, the leader in IGA, have joined forces to deliver an integrated solution that extends governance into the unmanaged realm of shadow SaaS. By combining SailPoint's advanced governance capabilities with Grip's robust SaaS discovery and risk mitigation technologies, this partnership empowers organizations to achieve comprehensive visibility and control over their entire SaaS ecosystem. Together, they address a broader spectrum of identity and SaaS-related risks, providing a unified approach to governance and security that maximizes the strengths of both solutions.

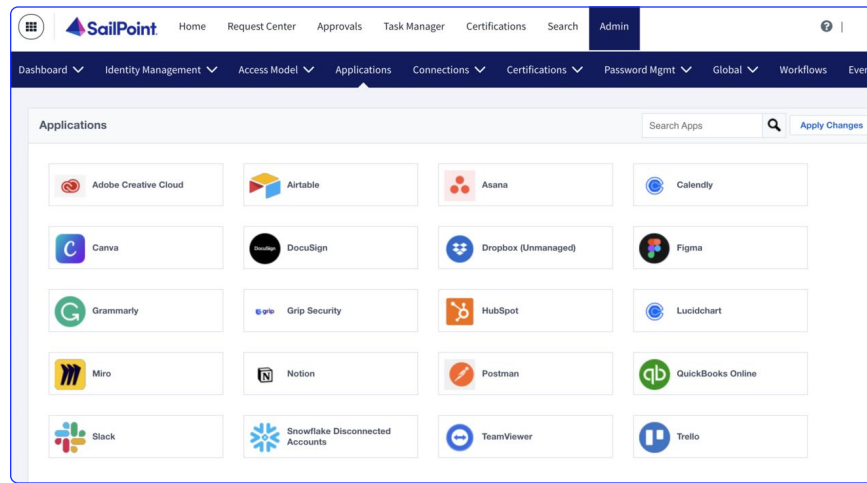
By integrating Grip and SailPoint, organizations unlock the following capabilities:

### Visibility of All SaaS, Including Shadow SaaS

- **Comprehensive App Discovery:** Identify all SaaS applications in use, both managed and unmanaged, with seamless visibility in SailPoint's interface.
- **Actionable User Data:** Gain insights into the identities accessing these apps, including potential business owners, to ensure proper governance.
- **Detailed App and User Context:** Access vital information about discovered apps, which can be used to design more informed workflows in SailPoint.

## Key Benefits

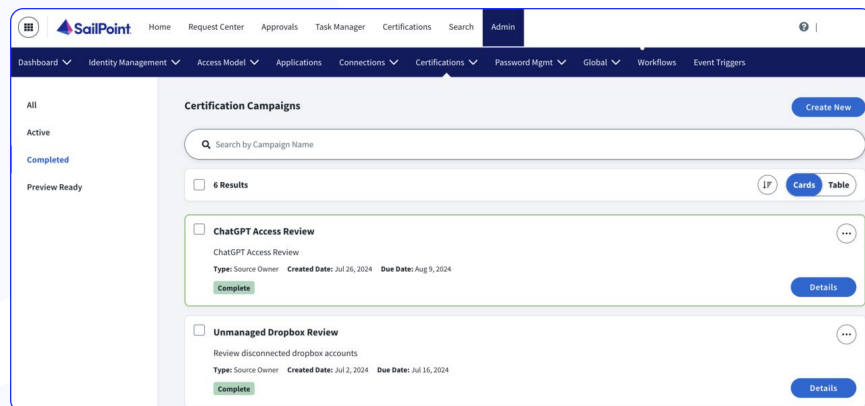
- **Increased Value of IGA Investment:** Govern and secure tens of thousands of SaaS apps, extending the value of your SailPoint solution.
- **Quick Time to Value:** Integrate with Grip in minutes to gain immediate visibility into shadow SaaS apps and users, allowing for governance workflows like access certification and access revocations on more SaaS apps.
- **Reduced Risk:** Minimize security risks by discovering shadow SaaS apps and taking actions like revoking access, delivering protection beyond the normal scope of IGA solutions.
- **Future-Proof Identity Management:** Safeguard your organization's access to both existing and future applications, fortifying security for the long term.



With Grip, SailPoint can see all SaaS apps and users in your environment.

## Extending Access Certifications to Shadow SaaS

- **Expanded Certification Scope:** Strengthen access certification campaigns by incorporating unmanaged shadow SaaS apps.
- **Efficient Management:** Involve business owners to manage access certifications at scale with higher accuracy.
- **Informed Decision-Making:** Leverage Grip's rich metadata on app type and governance status to make more informed access certification decisions.



Certify SaaS access with the appropriate business owners.

## Remediate Access to Shadow SaaS

- **Revoke Unmanaged App Access:** Utilize Grip's RPA-driven password rotation to revoke access to shadow SaaS apps that aren't directly connected to SailPoint.
- **Flexible Revocation Options:** Choose manual or automated revocation flows as part of employee offboarding or certification processes.
- **OAuth Scope Revocation:** Gain the ability to revoke unnecessary Google Workspace and Microsoft 365 OAuth scopes for apps identified as risky.

Identity: DiegoS@4acme.com

Actions

Details
Access
Accounts
Work Reassignment
Events

Accounts

Search Accounts

6 Results

| Name            | Native Id...   | Source N...        | Status   | Created                   | Modified                  | Act |
|-----------------|----------------|--------------------|----------|---------------------------|---------------------------|-----|
| Diego Siciliani | 4c6e00af-35... | Grip Security C... | Enabled  | Jun 5, 2024, 11:55:32 PM  | Sep 16, 2024, 9:44:46 AM  |     |
| Diego Siciliani | ca1f5699-16... | Entra Environ...   | Enabled  | Jun 3, 2024, 9:56:10 PM   | Jun 3, 2024, 9:56:11 PM   |     |
| Diego Siciliani | 4c6e00af-35... | Unmanaged D...     | Enabled  | Oct 30, 2024, 12:07:22 AM | Oct 31, 2024, 12:05:29 AM |     |
| Diego Siciliani | 4c6e00af-35... | Box                | Enabled  | Aug 6, 2024, 12:48:10 PM  | Sep 23, 2024, 7:38:49 AM  |     |
| Diego Siciliani | DiegoS@424...  | IdentityNow        | Enabled  | Jun 3, 2024, 9:56:11 PM   | Jun 3, 2024, 9:56:11 PM   |     |
| Diego Siciliani | 4c6e00af-35... | Snowflake Dis...   | Disabled | Jun 6, 2024, 11:12:59 PM  | Jun 28, 2024, 11:14:25 AM |     |

Rows per page
25
1 - 6 of 6
Page
1
of 1

Remediate and revoke access to more apps.

## Continuous Monitoring and Security

- **Ongoing SaaS Monitoring:** Continuously discover new SaaS applications and track changes in existing ones, ensuring ongoing compliance and security.
- **Dynamic Risk Scoring:** Monitor risk level changes in previously discovered and sanctioned apps to ensure ongoing alignment with security policies.
- **Proactive Security Automation:** Automatically trigger corrective actions for newly discovered or updated applications, ensuring comprehensive and up-to-date identity provider (IdP) coverage.

Accounts
diegos@acme.com ON Box

Actions

|                              |  |   |                             |
|------------------------------|--|---|-----------------------------|
| NAME<br>diegos@acme.com      | ID<br>25d35e4b02d34f0399ce09233dba1605 | NATIVE IDENTITY<br>4c6e00af-3586-4e9c-a36b-f915fc14fb0f | IDENTITY<br>diegos@acme.com |
| SOURCE NAME<br>Box           | MANUALLY CORRELATED<br>false           | STATUS<br>Enabled                                       | LOCKED<br>false             |
| PASSWORD LAST CHANGED<br>--- | CREATED<br>Aug 6, 2024                 | MODIFIED<br>Sep 23, 2024                                |                             |

Pinned Attributes

Synchronize changes to SaaS into SailPoint for dynamic security and compliance.

This Grip-SailPoint integration empowers organizations to close the gap on shadow SaaS risks while extending the value of their identity governance efforts, creating a more secure and resilient enterprise ecosystem.



Grip Security is a pioneer in SaaS identity risk management, providing innovative solutions to help enterprises address the security risks associated with widespread SaaS adoption.

### Contact Us

✉ [info@grip.security](mailto:info@grip.security)

🌐 [@GripSecurity](https://www.GripSecurity.com)

🌐 [grip.security](https://www.grip.security)



SOC 2 Type II  
Certified



ISO 27001  
Certified