Data Sheet

Grip SaaS Security Control Plane

Discover Shadow SaaS and rogue cloud accounts. Prioritize identity sprawl risks. Secure unsanctioned SaaS and cloud accounts. Orchestrate risk mitigation and remediation.

SaaS Identity Risk Management

SaaS identity risk management (SIRM) is emerging as a critical pillar of cybersecurity to manage access to applications and cloud services. SaaS has created a world where data is stored everywhere and accessed from anywhere, and the effectiveness of traditional security control points, i.e., network, endpoint, or application, has eroded and no longer sufficient. SaaS identities have emerged as the ultimate control point and transcends the limitations of traditional control points.

More employees are working remotely using unfederated SaaS applications, and these services are beyond the enterprise perimeter. As a result, much of the SaaS employees use today are more susceptible to becoming a target that can be exploited by bad actors. The compromise of one system or app can be subsequently used to gain unauthorized access to other systems, apps, or resources, and this increases the company's exposure to security risks. With nearly 75,000 SaaS apps available, the adoption of SaaS continues to surge, and companies need to implement effective controls to manage the identity sprawl that is created.

SaaS Security Control Plane Capabilities

Key benefits & capabilities

Discover Shadow SaaS
Gain a complete picture of your SaaS landscape and risks. Monitor usage and login methods to both federated and unfederated apps.

Prioritize SaaS Risks for SSO Integration
Unified risk profile based on multiple factors including user adoption, data used, user roles, privileges, and app data sensitivity for prioritization for SSO integration.

Streamline SaaS Breach Remediation
Incorporate automated incident response capabilities that enable immediate action upon identifying security risks or policy violations.

Lower Licensing Costs
Identify redundant SaaS apps and enable SAML-less SSO without upgrading to enterprise license tiers and incurring the enterprise security tax.

Control Shadow SaaS Access
Regulate the use of shadow SaaS apps by implementing policies and procedures to control access.

Grip SaaS Security Control Plane

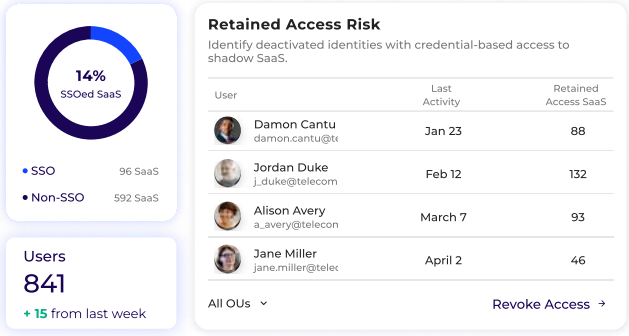
The Grip SaaS Security Control Plane (SSCP) is a robust cybersecurity platform specifically developed to deliver SIRM. It does this by strengthening an enterprise's identity security posture in the fast-paced landscape of SaaS and cloud services consumption. The Grip SSCP offers a range of features and capabilities that leverages identity as the control point for user access to SaaS and cloud services.

Unlike other SaaS security products, the Grip SSCP platform covers both federated and unfederated SaaS apps and streamlines security operations, reducing manual effort and improving response times to SaaS identity security risks. This unique combination enables proactive risk assessments, ultimately strengthening the company's defenses and improving security efficacy.

Discover All SaaS Usage

The Grip SSCP uses advanced email analysis and integrations with identity security systems to identify all SaaS being used and understand how users access them. The platform's proprietary algorithms can analyze emails and detect SaaS events gathered from additional systems to provide a comprehensive view of the security posture of SaaS identify risks.

- **Automatic Discovery:** Automatically discovery new and existing SaaS and cloud accounts for federated and unfederated apps and systems
- **Continuous Monitoring:** Constantly monitor for new account creation and alert security teams with recommended actions
- **Identify Inactive Accounts:** Reveal accounts that are dormant or inactive to be reviewed or reclaimed for redistribution

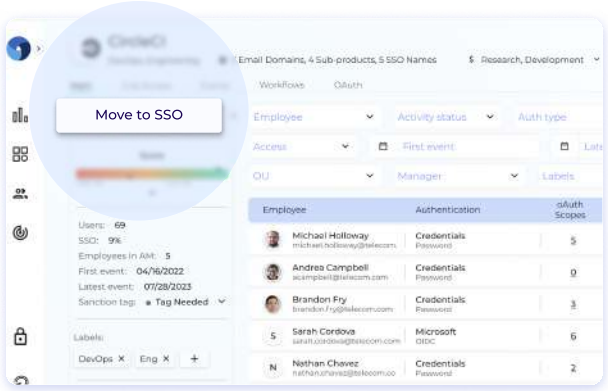


Shadow SaaS Discovery Metrics

Prioritize SaaS Identity Risks

The Grip SSCP integrates app data, user profiles, and account access behaviors to understand SaaS identity risks. This 360-degree view provides a unique risk profile of every user and SaaS app or cloud service, providing clear prioritization of the remediation or mitigation required.

- SaaS Risk Scoring and Prioritization: Assesses the severity and impact of SaaS apps and assign priority levels for risk mitigation
- Contextual Risk Assessment: Incorporates contextual information, such as user roles, privileges, and app data sensitivity, to provide a comprehensive risk assessment
- Threat Intelligence Integration: Integrate external threat intelligence sources to provide additional information about emerging identity risks



One-Click Move Shadow SaaS to SSO

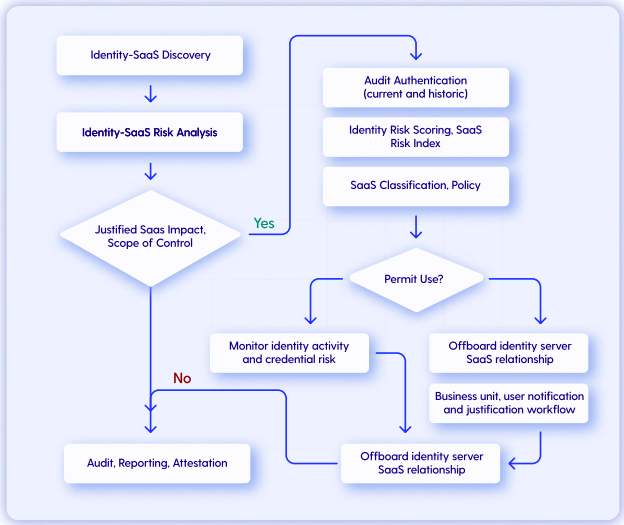
Secure Shadow SaaS And Rogue Cloud Accounts:

Security teams can utilize the Grip SSCP's robotic process automation (RPA) to secure access to unfederated SaaS apps and cloud services. The technology leverages the native password reset functionality of SaaS apps to take back control of an identity or secure access to the app.

- Control SaaS Access: Control and manage access to shadow SaaS and cloud accounts including app onboarding, deprovisioning, and access revocation
- Standardize Authentication: Enforce the use of identity systems, such as SSO, for users who are not using them or centralize user authentication to a common system for unfederated accounts
- Automate Account Security: Automatically lock or take over control of shadow SaaS or cloud services because of inactivity, non-compliance, or employee offboarding

Automated Offboarding

- SaaS Onboarding Automation: Require users to submit business justification for new SaaS to enforce risk and compliance policies
- Automate Identity Breach Response: Automate the discovery and renewal of credentials for affected users for unfederated SaaS apps and cloud services
- Enable Identity Access Control: Allow other security systems, such as EDR, CASB, firewalls, etc., to leverage identity as a control point to enforce policies



Automated Orchestration Workflows

Orchestrate Risk Mitigation Or Remediation:

Integrate the Grip SSCP with systems and tools to help streamline operations. The platform acts as a centralized hub to automate SIRM tasks such as user onboarding, offboarding, SaaS justifications, and remediation of user credential breach incidents for unfederated apps and systems.

Key Use Cases and Capabilities

Use Case and Feature	Description
Shadow IT Discovery	
SaaS use discovery	Identify every SaaS account created in real time. Works for managed and unmanaged devices.
Cloud services discovery	Discover rogue cloud service accounts for AWS, GCP, and Azure toidentify the users of each account
Shadow IT account alerts	Get alerts every time an employee creates a new unfederated SaaS or cloud services account
Consolidate Redundant Apps	
Standardize apps	Discover and move users off redundant apps to standard ones. For example, find users of Box or Dropbox and move to OneDrive.
Find shadow SaaS owner	Quickly identify the business or billing owners of shadow SaaS apps to understand business justification
Accelerate Incident Response	
SaaS breach remediation	Automatically rotate passwords to remediate SaaS breaches or protect the digital supply chain
Find SaaS owner	Identify the business and billing owner of shadow SaaS apps for incident response

Key Use Cases and Capabilities

Use Case and Feature	Description
SSO Integration	
Prioritize apps for SSO	Identify every SaaS account created in real time. Works for managed and unmanaged devices.
SSO enforcement	Discover rogue cloud service accounts for AWS, GCP, and Azure toidentify the users of each account
Shadow SaaS Authentication	
SAML-less SSO Governance	Enable SSO-like governance for shadow SaaS apps or those that do not support OAuth
Lower Licensing Costs	
Reclaim unused licenses	Discover licenses allocated to users who no longer use an app to reallocate to other users
Discontinue unused SaaS subscriptions	Find SaaS services that are no longer used to discontinue subscriptions or cancel
Prevent users from using redundant SaaS apps	Alert users who sign up for redundant SaaS apps and notify them of alternative, sanctioned apps

Data Sheet

Key Use Cases and Capabilities

Use Case and Feature	Description
Provide Visibility to Cloud Services	
Consolidate cloud accounts (AWS, GCP, Azure) into corporate tenants	Gain visibility into rogue cloud accounts that are not part of the corporate tenants
Cloud account creation alerts	Get alerts for newly created cloud accounts and ask users to justify reasons for creating them outside of corporate tenants
Automate SaaS on/offboarding	
SaaS onboarding	Detect new unfederated SaaS accounts and record it in software asset management systems
SaaS offboarding	Identify all shadow SaaS accounts for an employee and secure account access by blocking access
Shadow IT Justification	Automate business justification for shadow SaaS IT accounts from users