



Grip Extend

As organizations grow their digital operations, identity management has become a critical component of enterprise security. While processes for managing known applications and identities are often solid, shadow SaaS and unmanaged identities remain blind spots. These overlooked assets are prime targets for cyberattacks, particularly when weak or compromised credentials are involved. So, how can organizations address this gap and secure their SaaS environment?

The Solution: Grip Security

Grip Security solves the challenge of shadow SaaS with its SaaS Identity Risk Management (SIRM) platform, which combines powerful discovery with proactive risk mitigation. Grip's discovery engine uncovers unmanaged applications outside of IT's control and enables security teams to take swift action, reducing threats and securing the entire SaaS ecosystem.

Overview of Grip Extend

Grip Extend builds on the core platform, adding advanced features through a lightweight browser extension. This extension gives security teams greater visibility and control over SaaS risks, from identifying credential hygiene issues to monitoring real-time shadow SaaS usage. It also discovers applications that don't send email notifications, like user portals, and allows direct communication with users through the browser.

Key Capabilities

Credential Hygiene Risk Discovery: Identify users with weak, reused, or compromised credentials, helping security teams prioritize remediation efforts and improve identity hygiene.

Top Vulnerable Identities			
Display at risk identities by total number of vulnerable accounts. ⓘ			
Identities	Weak Passwords	Reused Passwords	Compromised Passwords ⓘ
YS Yvette Strong ys1@acme.com	2	35	3
NZ Norm Zimmerman nz1@acme.com	14	27	14
JE Jerry Ellwood je@acme.com	4	21	4
YS Yana Smith ys2@acme.com	2	20	2
RK Rebecca Kerry rk@acme.com	3	19	4

[Download Report →](#)

Shared Account Detection: Detect shared accounts, enabling better access management, enforcement of secure password practices, and safer methods of account sharing.

Shared Accounts
Highlight top shared accounts in the organization by identities count.

App Name	Username	Identities	Password Strength
JAMF	admin1@acme.com	RS OR ZY +49	Strong
Zendesk	admin2@acme.com	BH YS KG +42	Strong
LinkedIn	admin3@acme.com	GS EB BB +38	Strong
X	admin4@acme.com	YS JM BB +23	Strong
GitLab	admin5@acme.com	BH BB OR +22	Strong

[Download Report →](#)

Newly Introduced Apps
Discover the most recently applications introduced into your organization.

App Name	Source	First Discovered	Total Accounts	Risk Score
Zapier	Extension	Jul 1, 2023	18	64
Monday.co...	Extension	Jul 1, 2023	34	87
IBM	Email	Jul 1, 2023	87	18

By Apps ▾ Last 30 days ▾ [Explore More →](#)

Shadow SaaS Identification: Discover hard-to-find shadow SaaS applications, such as portals that don't send email notifications, ensuring complete visibility into SaaS usage.

Real-Time Detection: Monitor user authentications in real time, flagging shadow SaaS activity and verifying the use of MFA. This empowers teams to enforce MFA when necessary.

High Risk Unmanaged Apps Without MFA
Monitor high-risk applications within the organization that are not configured with multi-factor authentication.

App Name	Risk Score	Total Accounts
Asana	78	19
Circle CI	82	8
Logz.io	83	78
OpenAI	96	89

All OUs ▾ [Download Report →](#)

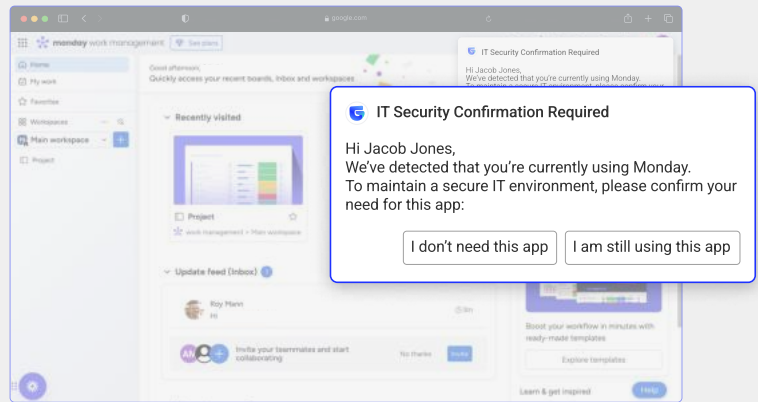
Inactive Apps
Evaluate inactive or underused applications within your organization.

App Name	Accounts	% Usage
Asana	174	5%
Smartsheet	103	9%
Zapier	97	12%

By Apps ▾ Last 30 days ▾ [Download Report →](#)

Stale Account Detection: Identify and remove inactive accounts in shadow SaaS, reducing risk and reclaiming unused resources.

In-Browser Communication: Directly engage users through the browser, prompting them to explain or justify new SaaS usage, encouraging better security practices and reducing the spread of unmanaged apps..



Benefits

- **Reduce Breach Risks:** Enforce strong passwords and MFA across the SaaS ecosystem to prevent breaches.
- **Data-Driven Security Decisions:** Gain detailed insights into credential hygiene, enabling proactive risk management.
- **Secure Shared Accounts:** Protect shared accounts, such as those used for social media or collaboration tools, safeguarding security and brand reputation.
- **Manage Shadow SaaS:** Identify and transition unmanaged SaaS apps into a managed state, reducing risks and improving oversight.
- **Eliminate Stale Accounts:** Detect and offboard inactive shadow SaaS accounts, optimizing licensing costs and minimizing exposure.

Privacy Considerations

Grip Security takes privacy seriously. Grip Extend only monitors work-related activities, with configurable settings to ensure compliance with organizational policies. It does not track personal browsing habits, collect emails, or store passwords.

Requirements/Setup

Deploying Grip Extend is seamless, requiring the installation of a browser extension. IT teams can distribute the extension via Group Policy Objects (GPO) for easy integration into existing workflows. The Grip Portal also offers customizable options, allowing organizations to adjust data collection based on their specific needs.



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

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

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



SOC 2 Type II
Certified



ISO 27001
Certified