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.

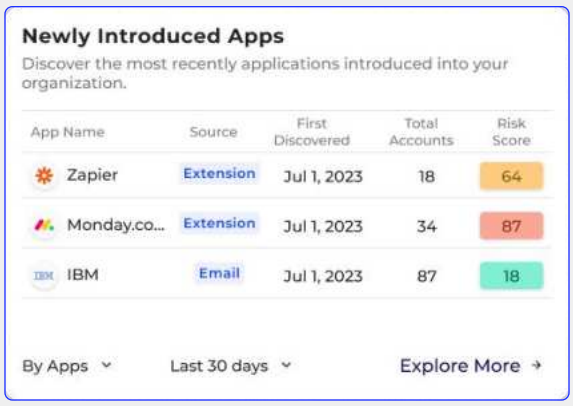
Overview of Grip Extend

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.

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

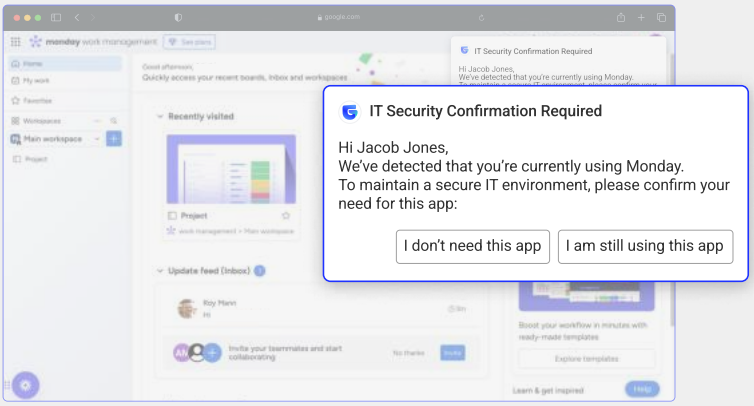


Shadow SaaS Identification: Discover hard-to-find shadow SaaS applications, such as portals that don't send email notifications, ensuring complete visibility into SaaS usage.

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.

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.

Contact Us

info@grip.security

@GripSecurity

grip.security