Extend User Security

Secure one of the most vulnerable aspects of SaaS security: user-managed identities.

Strengthen User Security Across All SaaS

As organizations increasingly rely on SaaS, corporate identities face growing security risks beyond traditional protections. While identity providers (IdPs) enforce SSO, MFA, and account lifecycle management, these safeguards don't cover unmanaged SaaS applications, including shadow SaaS, leaving accounts vulnerable. Without centralized security oversight, users unwittingly put corporate identities at risk by using weak passwords, reusing credentials across apps, neglecting MFA, or logging into unsafe applications—creating prime opportunities for credential theft, account compromise, and cyberattacks.

Grip Extend User Security bridges this gap by extending security controls to unmanaged and unknown apps, ensuring corporate identities remain protected. It provides security teams with critical visibility and control, integrating seamlessly with the Grip SaaS Security Control Plane to deliver real-time insights into SaaS usage, MFA adoption, credential hygiene risks, and more. Additionally, Grip Extend engages users directly in the browser, guiding them away from risky behaviors before exposure occurs. With Grip, organizations can proactively secure corporate identities across their entire SaaS ecosystem.

Why Grip Extend User Security?

Grip Extend User Security closes a critical gap in SaaS security by protecting unmanaged applications beyond IdP controls. By offering deeper insights into these apps via the Grip SaaS Security Control Plane and interacting with users at the browser level, it enables organizations to strengthen security best practices—such as MFA and strong credential hygiene—while mitigating risks without disrupting workflows.

Outcomes Achieved

- **Reduce Breach Risks**
  Enforce strong passwords and MFA across the SaaS ecosystem to prevent unauthorized access.
- **Make Informed Security Decisions**
  Gain detailed insights into credential hygiene for proactive risk management.
- **Secure Shared Accounts**
  Protect shared accounts, such as those used for social media or collaboration tools, preserving security and brand reputation.
- **Eliminate Stale Accounts**
  Detect and offboard inactive shadow SaaS accounts, optimizing licensing costs and minimizing exposure.
- **Encourage Safer User Behavior**
  Proactively guide users to avoid risky actions, such as using weak credentials for authentication.

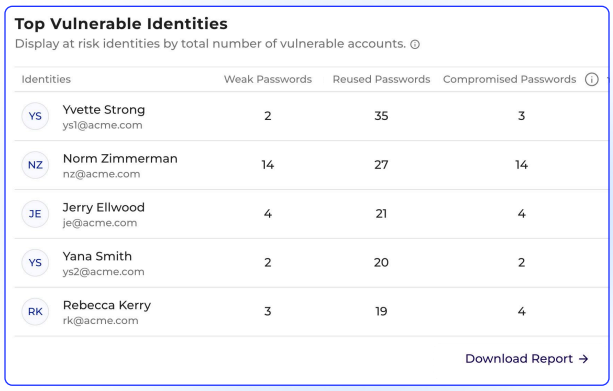
Key Features:

- Credential Hygiene Risk Discovery
- Shared Account Detection
- MFA Detection
- Stale Account Detection
- User Portals and Other Apps Detection
- In-Browser Communications

Key Feature Details

Credential Hygiene Risk Discovery

Identify users with weak, reused, or compromised credentials, helping security teams prioritize remediation efforts and improve identity hygiene, especially in non-federated SaaS apps.

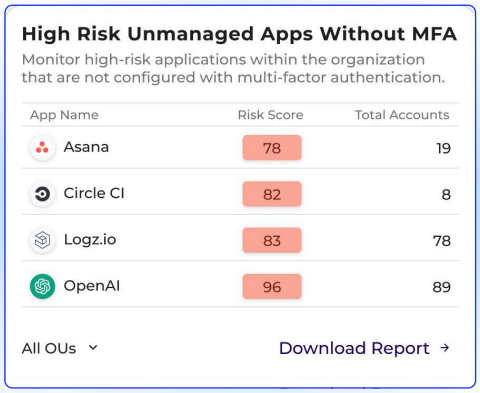


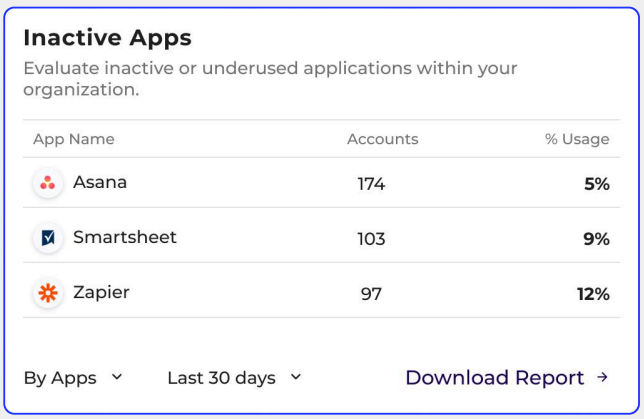
Shared Account Detection

Detect shared accounts to enhance access management, enforce secure password practices, and promote safer methods of account sharing.

MFA Detection

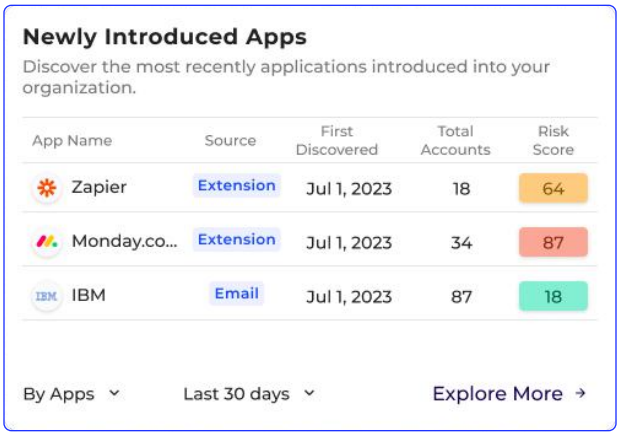
Monitor user authentications to flag SaaS apps without MFA, empowering teams to enforce MFA authentication policies where needed.





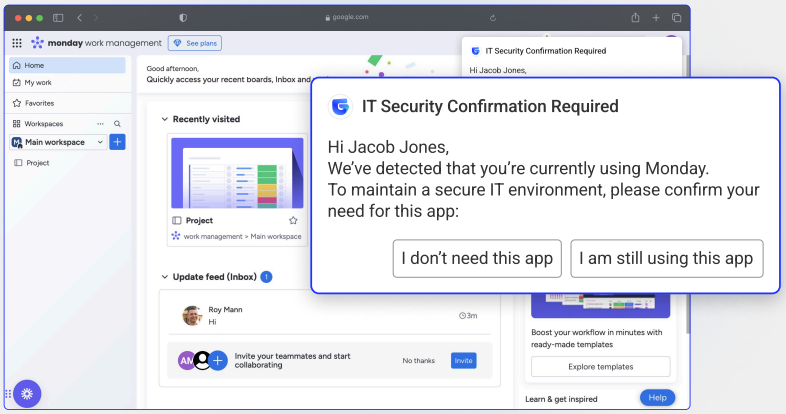
Stale Account Detection

Identify and remove inactive accounts in shadow SaaS, reducing risk exposure and reclaiming unused resources.



User Portals and Other Apps Detection
Discover additional applications, such as user portals that may not send user emails, ensuring comprehensive SaaS visibility.

In-Browser Communications
Prompt users directly in the browser to justify new SaaS usage, enhance credential security, avoid unsafe applications, and reinforce corporate identity protection.



Privacy Considerations

Grip Security prioritizes privacy. Grip Extend User Security 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 User Security is seamless, requiring only the installation of a browser extension. IT teams can distribute the extension via Group Policy Objects (GPO) for easy integration into existing workflows. Grip offers customizable options, allowing organizations to adjust data collection according to their specific needs.

grip

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
grip.security

SOC 2 Type II Certified

ISO 27001 Certified

© Grip Security, Inc. 2025. All rights reserved.