Reco
Secure Your SaaS

Ensure the Right Access – And Not More

Inadequate access and privilege management can lead to unauthorized access and security risks. Understand critical exposure gaps from user permission level and behavior in your SaaS ecosystem that can lead to a breach.

Discover Critical Exposure Gaps

We unify identities across SaaS apps so you can discover admins, over-permissioned users & service accounts. Understand critical exposure gaps from stale accounts and MFA violations that can lead to a breach.

Pinpoint & Revoke Permissions

Assess the risk associated with current users' access using least privilege access, including inactive users, external users, and non-admin roles. Pinpoint and revoke permissions that are unused or dormant.

Monitor for Over-Privileged Users

Understand who is using your SaaS apps, their app permission level and whether they are over-privileged, an Admin, or a former employee with access. Determine access to critical data and whether they can perform harmful actions.

Automate Continuous Access Reviews

Initiate continuous access reviews with relevant stakeholders in your organization to certify entitlements across your SaaS apps. Generate reports on access status and deprovisioning activities for audits.

Posture Management & Continuous Compliance

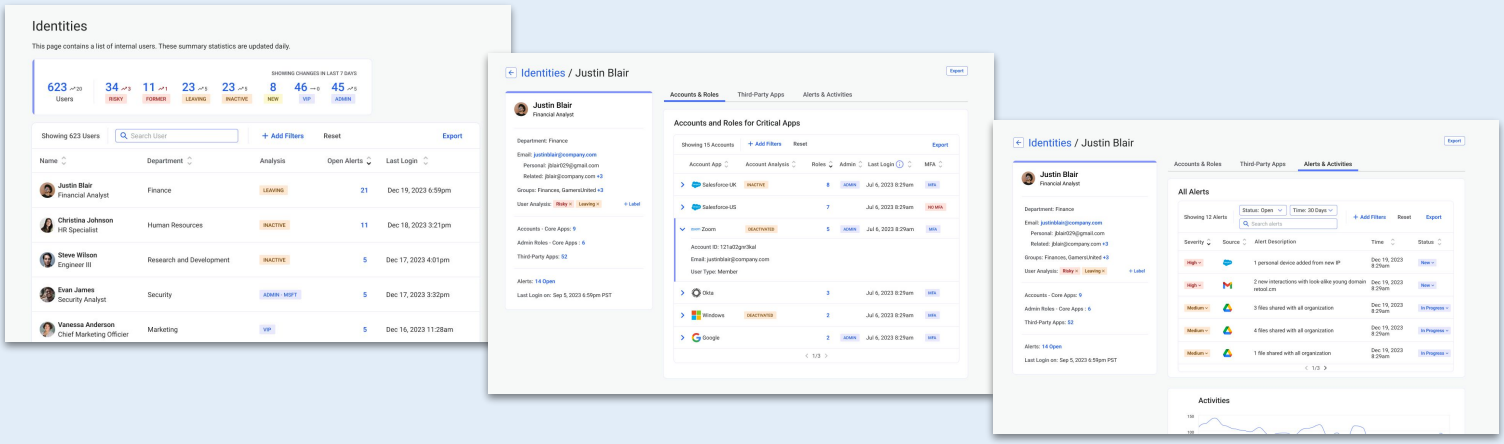
App Discovery & Governance

Identity & Access Governance

SaaS Detection & Response

Context You Need to Prioritize Risk

Reco uses advanced analytics around persona, actions, interactions and relationships to other users, and then alerts on exposure from misconfigurations, over-permission users, MFA violations, stale accounts, and risky user behavior. Use this comprehensive picture to empowers your Security team to prioritize the most critical points of risk.



Reco Continuously Monitors for Potential Data Exposure in Identities

100B+
user identities analyzed

70%
cost savings from inactive/unused licenses

80%
of indicators of compromise based on identity-based attack methods

Reco Supports These Business-Critical SaaS Applications and More

Microsoft 365 · Google Workspace · salesforce · zoom · slack · okta · GitHub · box · WIZ · ATLASSIAN · monday.com · NetApp

Organizations Worldwide Trust Reco to Control User Access

CISO, Marketing Analytics Software Company: “Reco detected insider risk of a leaving employee snooping and downloading excessive files from Salesforce. We were able to address this quickly.”

Tomer Stenzler, Director of Cyber Security: “There was a new member of the IT team that automatically received Admin privileges in the SSO provider, and granted them IT admin privileges to Salesforce, Github, Netsuite. They didn’t need those high privileges to do their job, and just inherited it. Reco informed us of this situation so we could revoke access.”

solaredge

To learn more, email us at **info@reco.ai** or visit **reco.ai.**