SCIRGE

SHEDDING LIGHT ON SHADOW IT

www.scirge.com
hello@scirge.com

At a Glance

Scirge provides a unique approach to unveil and gain control over unmanaged third-party web accounts.

It reveals unknown web apps and manages password hygiene issues such as shared accounts, weak passwords or account reuse for employees using corporate email addresses as credentials.

Scirge enables you to have control and visibility over your company's SaaS usage to help you comply with GDPR and other audit requirements, effectively reducing the IT operational overhead and cost relating to unsanctioned Shadow IT usage.

> ***CIOs underestimate the number of cloud applications by a factor of 15-22x***
> ***— Cisco***

Account Protection and Awareness

Cloud Web App Inventory and Intelligence

Compliance and Risk Assessment

Our Mission

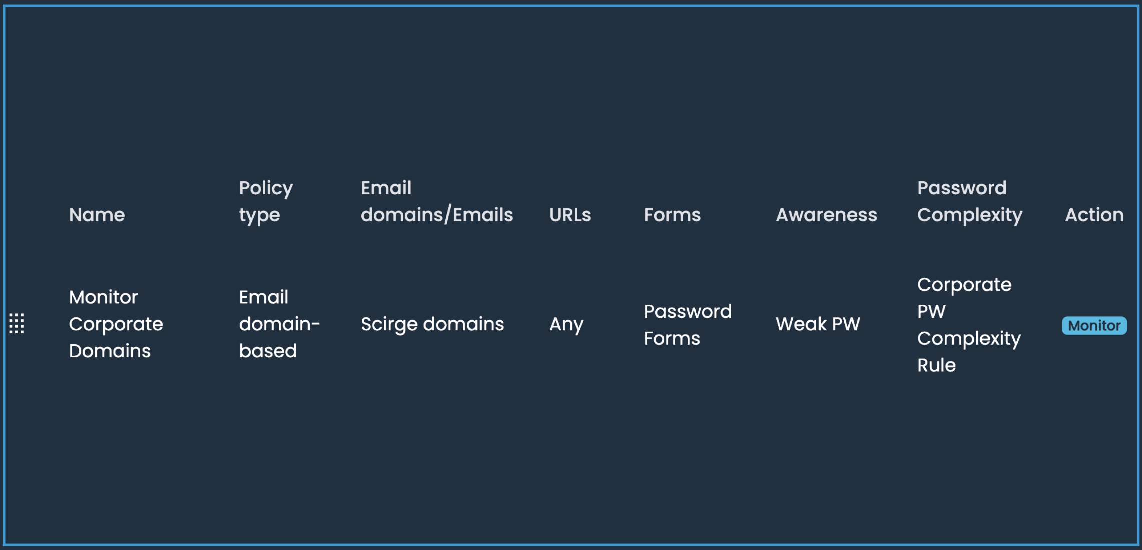
We founded Scirge to fill a gap in the IT Security and Management field. Scirge specializes in helping modern organizations discover, secure, and manage their cloud footprint.

Our mission is to reduce management overhead, facilitate compliance, and reduce exposure to credential-related threats.

We do that with our innovative, high-quality software and services while remaining agile, fast-moving, and customer-friendly.

Scirge Workflow

Scirge is easy to deploy and manage. The Central Server is responsible for management, while the Endpoints collect information from Chrome, Edge or Firefox browsers. Based on centrally-managed policies, Scirge monitors and collects company-related credentials and all relevant information from the given website to build a local inventory for your cloud security purposes. Users may be alerted or redirected for awareness training when they are at risk of breaching certain policies. Scirge works locally and even offline, building a local app and account directory for organizations based on the actual usage.



Name	Policy type	Email domains/Emails	URLs	Forms	Awareness	Password Complexity	Action
Monitor Corporate Domains	Email domain-based	Scirge domains	Any	Password Forms	Weak PW	Corporate PW Complexity Rule	Monitor

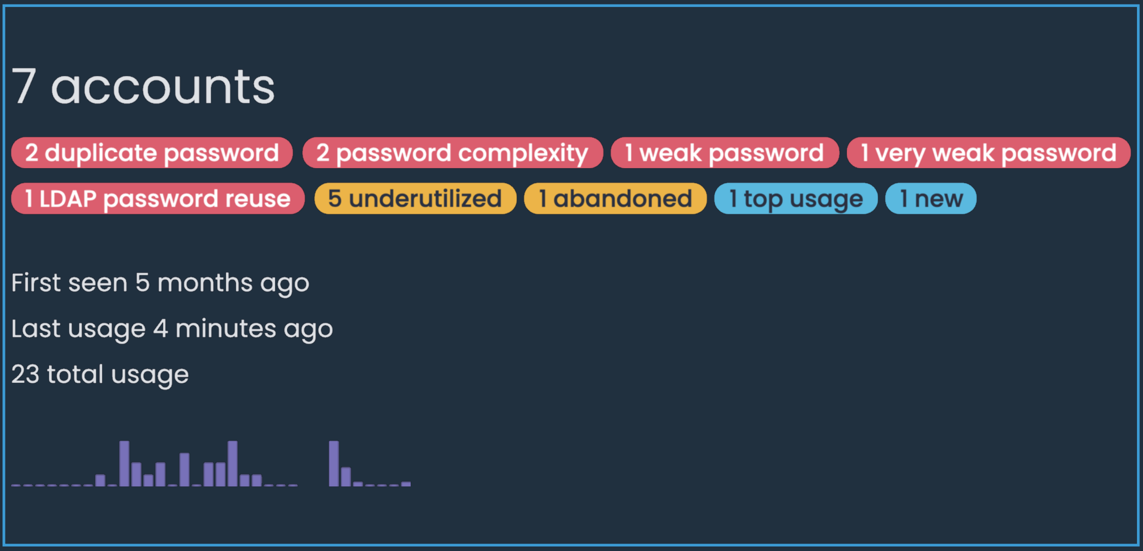
Key Features

- Role Based Access Control
- 4-eye principle
- Audit Logs
- PII Anonymization
- Endpoint Authorization
- Double-Encrypted communication

Account Protection and Awareness

The Scirge Endpoint can perform password hygiene checks, allowing it to discover if passwords have been reused from other cloud apps or your active directory. Red flag events are pinpointed, and alerts to users and security administrations can be configured. Scirge also tags shared accounts that are used by more than one employee, as well as accounts that seem to be abandoned by users.

> ***43% of all login attempts across the web are brute force attacks using vast databases of stolen accounts.***
> ***— Akamai***



7 accounts

2 duplicate password | 2 password complexity | 1 weak password | 1 very weak password | 1 LDAP password reuse | 5 underutilized | 1 abandoned | 1 top usage | 1 new

First seen 5 months ago

Last usage 4 minutes ago

23 total usage

Key Features

Centrally-managed policies based on:

- Corporate Email Domains
- Corporate Email Addresses
- Target URLs

Password Hygiene Checks:

- Password Complexity Validation
- Password Strength Metering
- Password Reuse Detection (AD/Web)
- Password Autofill Detection
- Password Expiration Tracking

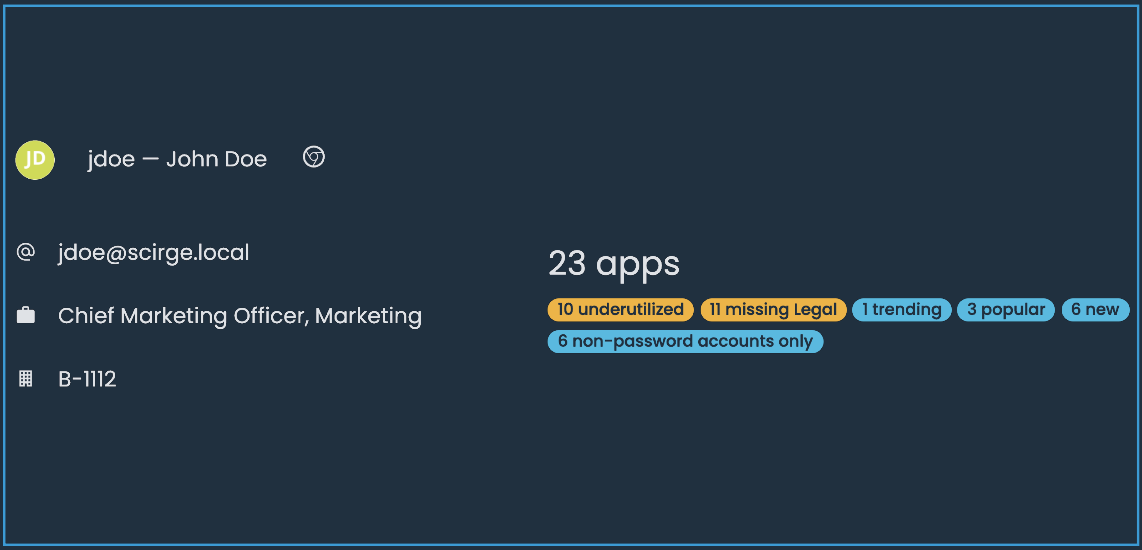
Awareness and User Education:

- Popup Message
- Banner Message
- Browser Redirection
- Multiple Trigger Rules

Cloud Web App Inventory and Intelligence

Scirge helps to track corporate cloud web app usage in order to create a full inventory of SaaS and cloud apps that account for costly Shadow IT spending and operational overheads. Scirge enumerates accounts for each web app and helps IT administration to understand the who, what, when and where of Shadow IT for the first time.

> ***The average person uses some 191 services that require them to enter passwords or other credentials.***
> ***— Digital Shadows***



JD jdoe — John Doe

@ jdoe@scirge.local

Chief Marketing Officer, Marketing

B-1112

23 apps

10 underutilized | 11 missing Legal | 1 trending | 3 popular | 6 new | 6 non-password accounts only

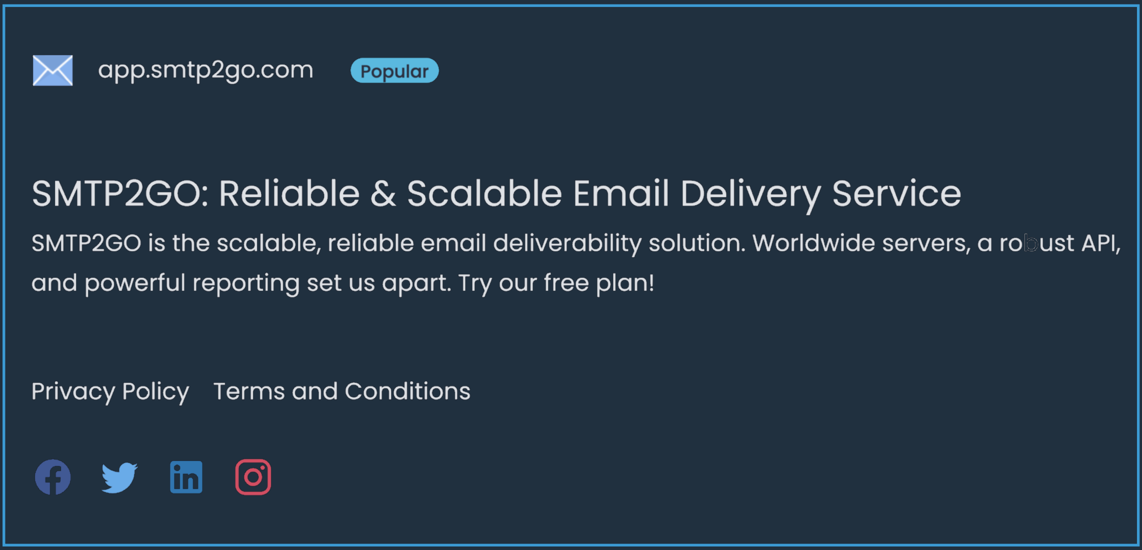
Key Features

- Detect any web app
- Automatic metadata collection
- User level app and account inventory
- Abandoned app and account detection
- Underutilized app and account detection
- Trending and Popular app tagging
- Application usage intelligence
- First and last access timestamps

Compliance and Risk Assessment

Scirge's automatic app data collection includes the privacy terms from each web application accessed by users. Privacy and compliance managers have the ability to review the terms of heavily-used apps to include them in risk assessments, business continuity and other policies, ensuring that they comply with GDPR, CCPA, ISO, NIST or other regulations and frameworks.

> ***Shadow IT presents a special problem in that these resources are enterprise-owned but not managed like other resources.***
> ***— NIST's Zero Trust Architecture***



app.smtp2go.com Popular

SMTP2GO: Reliable & Scalable Email Delivery Service

SMTP2GO is the scalable, reliable email deliverability solution. Worldwide servers, a robust API, and powerful reporting set us apart. Try our free plan!

Privacy Policy Terms and Conditions

Key Features

- Automatic Privacy Policy collection
- Automatic T&C collection
- Shared account detection
- AD Password Reuse Detection
- User authentication
- Central Web Application Inventory
- Blocking capability

SCIRGE

UNVEIL + CONTROL ALL BUSINESS WEB APP REGS & LOGINS

www.scirge.com
hello@scirge.com