SCIRGE
UNVEIL + CONTROL ALL BUSINESS WEB APP REGS & LOGINS

THE CHALLENGE OF SAAS MANAGEMENT

Businesses rely heavily on third-party web-based apps and services. Countless online accounts are created and used by employees each day on SaaS (Software as a Service) cloud platforms to tackle each task that the business requires. For instance, the marketing team has access to newsletter services, online creative tools, and social media tools; HR has access to job portals and HR software; the sales team utilizes CRMs and lead generation tools. Most of these accounts are created ad-hoc by employees, which means that they are unmanaged and unknown, creating a tremendous amount of risk and IT management overhead.

DID YOU KNOW?

On average, companies use hundreds of SaaS apps. Each employee has tens of individual SaaS accounts. This results in thousands of self-serviced, unmanaged accounts.

Shadow IT refers to resources utilized without the knowledge of the company's IT department. This can include hardware and software, though it mainly refers to cloud-based SaaS applications. Shadow IT is a hotbed for malicious activity against corporate resources.

- ✕ Unlike corporate accounts—such as Active Directory (AD)—these are mostly unknown to IT.
- ✕ If employees leave the company, they may still have access to these accounts.
- ✕ Users don't like passwords—they tend to either use weak ones or reuse corporate credentials.
- ✕ According to reports, billions of accounts are breached every year.
- ✕ Leaked credentials can be used to gain unauthorized access to corporate resources.
- ✕ Breaches and password reuse are the main culprits for account takeover (ATO) attacks.
- ✕ These accounts are often shared among employees, creating ownership issues.
- ✕ If an audit is required, it's almost impossible to manually collect the usage data of web accounts.
- ✕ The vast majority of such accounts are used for short periods, left unused and unmonitored forever.
- ✕ Overlapping and orphaned accounts can result in unnecessary expenses.

Scirge provides a unique approach to unveil and gain control over unmanaged third-party web accounts. Scirge tracks the websites employees use corporate email addresses to register on and log in to. Having a central dashboard of discovered accounts helps to reduce the risk of credential-related threats. It helps to ensure that your company complies with GDPR and other audit requirements.

MEET SCIRGE

Your Online Business Web App Account Officer

Discover

Scirge helps you track what web apps and services are being used within the company. New signups and existing account logins can both be detected.

Inventory

Scirge provides a central repository of discovered accounts used by employees. This helps to increase control over Shadow IT.

Control

With Scirge, centrally-managed and distributed policies dictate if an account can be used to register or to log in on a certain website.

Policies

Policies define what is monitored or blocked by Scirge. This can be selected based on numerous criteria that can be defined individually for each policy.

Awareness

The goal and one of the major features of this service is to educate. Scirge can display various centrally-configured messages upon policy matches.

Analytics

Data shown on the dashboard can reveal online web app account registration and log in metrics to help to make decisions.

HOW DOES IT WORK?

Scirge is easy to deploy and manage. Corporate SaaS accounts can be tracked down and discovered quickly.

Endpoint Browser Extension

A browser extension is deployed to endpoints, which can be done manually or centrally (via GPO, for instance). The Endpoint Browser Extension component fetches active configuration and policies and monitors the web account registrations and logins based on those specifications. It might block such action or warn the user; alternatively, it can silently log or ignore the action.

Central Server

The browser extension securely communicates with the Central Server to fetch active configuration and policies in order to send logs back. The Central Server collects, stores, and processes the data to provide useful, detailed log entries and analytics. The Central Server is where Administrators and IT Security Officers can create policies to set the behavior of the system.

Evaluation and Update

As time goes and data is collected and analyzed, policies can be fine-tuned to match the environment and business needs. There are numerous options to specify the policies—creating exceptions and global catch-all rules is simple. The Awareness module can be used to create educational messages for users to better understand the importance of proper account management.

WEB www.scirge.com

EMAIL info@scirge.com

SCIRGE