SCIRGE

SHEDDING LIGHT ON SHADOW IT

Shadow IT accounts and web applications create an unmanaged attack surface, operational inefficiencies, and compliance threats.

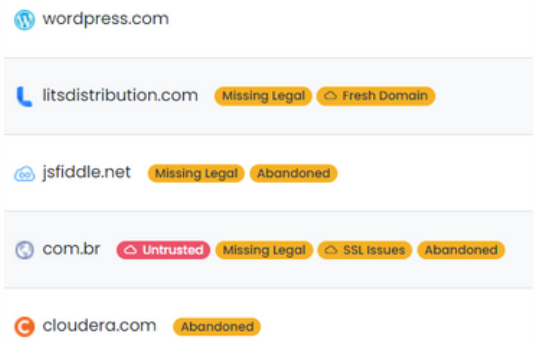
Scirge helps IT and Security decision makers to gain visibility into the digital supplychain, protect unmanaged accounts, reveal identities, and leverage context for compliance and operations.

Shadow IT Visibility

Scirge identifies SaaS and cloud web applications via a managed browser-extension. Detection is based on corporate email domains that were used for logging in on any website.

Application URLs are enriched via metadata collected from the browser, as well as dynamic data such as the domain age, blacklist checks, and other related intel.

This allows Scirge to build an inventory of all third-party applications without a database of known apps.

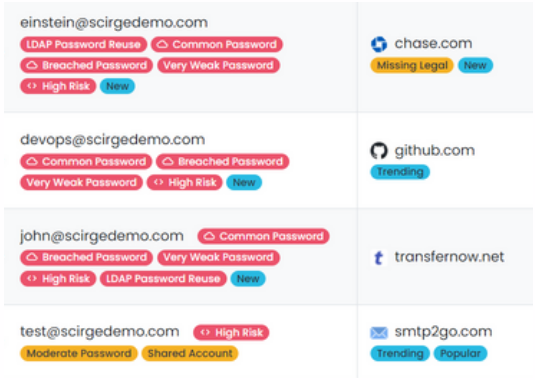


Applications Inventory

Account and Password Protection

Employee-created accounts are the Achilles' heel of every organization. Scirge monitors each password entered into a browser to prevent common attack vectors such as account takeovers, phishing, ransomware deployments, and fraud.

Custom complexity rules are available to match regulatory requirements while industry-standard secure hashing is used to detect password reuse, password sharing, and breached passwords.



Accounts Inventory

Active Directory Password Hygiene

AD/LDAP passwords go through the same process as any other account, enabling complexity checks for compliance and protection.

Identifying AD passwords that were reused in third-party web applications is a red flag, as stolen credentials contribute to 80% of successful attacks, including for ransomware deployments.

Instant Discovery

Scirge Discovery is a lightweight feature that helps organizations immediately assess their historic Shadow IT footprint via analyzing browser histories and browser-saved accounts.

This allows an audit and assessment of Shadow IT without any product integration. Reports will show the number of apps discovered and saved accounts will reveal exactly which apps and passwords may be vulnerable.

More About Use Cases

Compliance and Risk

Unmanaged third-party T&Cs and policies are enumerated along with geographic and trust-based data, to give context for risk assessments and audits.

Automated warnings and reports allow stakeholders and GRC professionals to stay updated about the emerging Shadow IT assets within the organization.

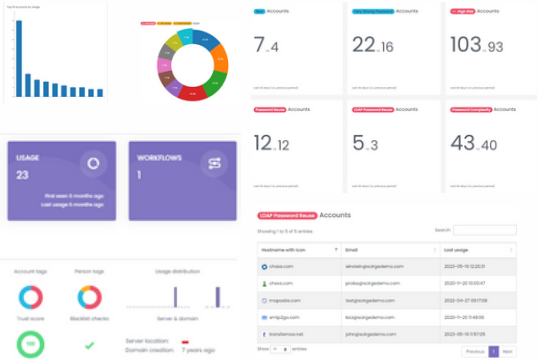
Visibility into account sharing and usage trends allows the early detection of misconduct or internal fraud. Offboarding processes are extended to unsanctioned services and identities.

Employee Education

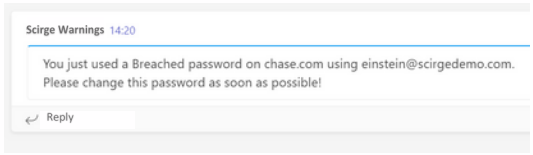
Distinct departments, experience, and professional backgrounds require a different approach to education. Scirge allows you to customize your educational messaging based on the triggers as well as your audience.

Warnings for poor password hygiene in IT departments may require added emphasis, while complexity requirements for non-IT professionals should be extremely clear and simple.

Resources



Custom Reports



Multi-channel messaging

Deployment Options

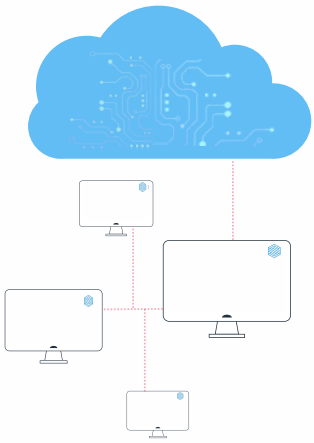
Scirge has a light endpoint component in the form of a browser extension. Its task is to monitor account and application usage via corporate emails and credentials and perform actions based on centrally-managed policies.

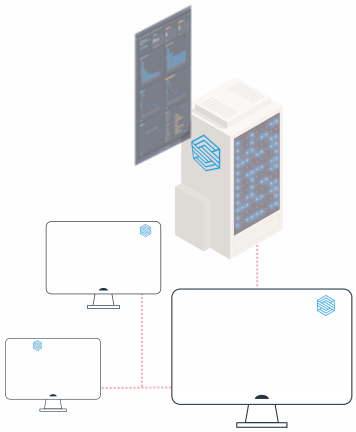
Management and configuration are available as a native cloud service or as an on-prem appliance. Managed Service Option is also available depending on your region. Horizon Cloud Intelligence services are available in all cases for data enrichment.

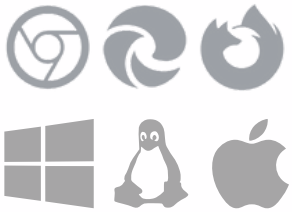
Chrome, Edge, and Firefox browsers are supported on all major endpoint operating systems.

	Virtual Appliance	Scirge Cloud (SaaS)	Managed Service
Perpetual (license + annual support)	●		
Subscription (single or multi-year)	●	●	
Monthly Billing (based on usage)			●

Deployment and licensing matrix







Security and Privacy

Endpoints collect a limited set of data governed by managed policies. Cleartext passwords are never stored, hashing and encryption at the endpoints, in transit, and on the server ensure the highest standards for data protection and privacy.

Read more about privacy and security.

Start a Trial

Board

Shadow IT discovery helps unveil the least known corners of an organization's IT footprint and supply chain. Scirge brings education that targets behavior, and early warnings for emerging threats.

IT Executives

Agility and digitalization can not happen without individual initiative. Silos in business units can not share knowledge, while IT needs visibility to support innovation by non-IT departments.

Shadow IT discovery helps reveal emerging trends and legacy or abandoned services that need attention from support, security, or financial aspects.

Risk and Compliance

Regulations and security frameworks are founded upon the inventory of your assets and their risk-to-value profile. Shadow IT is completely out of reach for risk analysis without specific, targeted efforts to create visibility.

Scirge enumerates inventories of unmanaged applications and accounts and adds context to their usage and risks. Tailor-made, awareness messaging helps improve the security habits of employees with varying tech skills and backgrounds.

Security Departments

Credential reuse and misuse are the number one contributor to ransomware deployment and successful breaches. Most unmanaged passwords and identities emerge from Shadow IT, where modern authentication methods can not be enforced.

Book a 30 minute Call