SHEDDING LIGHT ON SHADOW IT

Web Appllication Inventory and Intelligence
Account Protection and Awareness
Compliance and Risk Assessment

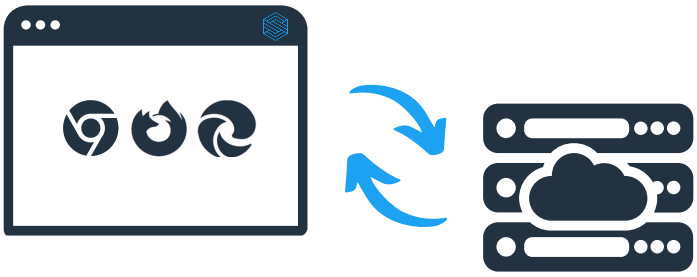
SCIRGE

Product Brochure for Version 3.0

hello@scirge.com

AT A GLANCE

Scirge provides a unique approach to unveiling and gaining control of unmanaged third-party web applications used by employees or business units, without the oversight of IT or security departments.



ARCHITECTURE

Scirge is easy to deploy and manage. The **Central Management Server** (CMS)—deployed as a local Virtual Appliance—is responsible for the management, while information is collected from Chrome, Edge, or Firefox browsers via our **Endpoint Browser Extension** (EBE), without needing a full-blown endpoint agent.

ENRICHED INVENTORIES

Data collected on the CMS is enriched with usage-related metadata based on custom threshold values and rules. Accounts and password hashes are correlated to discover password reuse, account sharing, and indicators of potential internal fraud or misconduct, all without ever storing cleartext passwords. Intelligence comes into play in the form of easy-to-read tags that can be used for correlation and investigation.

POLICY-BASED WORKFLOW

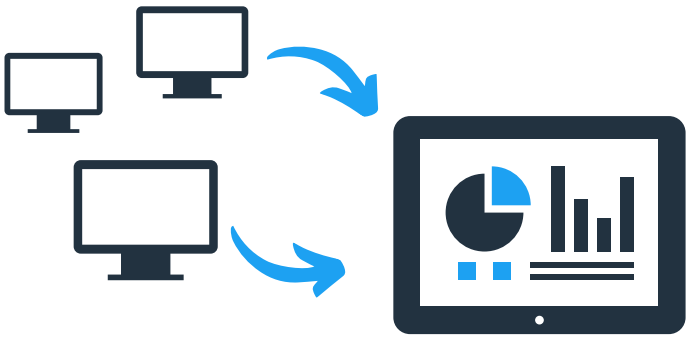
The Scirge EBE monitors and collects company-related credentials and all the relevant information from websites, and it does this based on centrally-managed policies. Users may be warned or redirected to awareness training via in-browser alerts when they are at risk or if they breach policies.

CLOUD INTELLIGENCE

With the help of the **Horizon Cloud Intelligence** (HCI) service, further metadata enrichment is available, including domain reputation and blacklist checks. HCI also verifies password hashes against known breach databases and common password lists, further securing your accounts against account takeover attempts and brute-force attacks.

WEB APP INVENTORY AND INTELLIGENCE

Scirge creates a full inventory of SaaS and cloud apps that pose potential risks in terms of compliance and data leaks. Enumerating the accounts for each web app helps you and your teams to understand the who, what, when, and where of Shadow IT.



CLOUD CONSUMPTION TRENDS

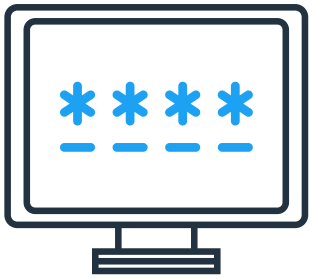
Configurable tags with custom thresholds give you insight into application usage trends amongst all employees. Underutilized or abandoned applications unveil changes in business requirements or unnecessary subscriptions. Overlapping subscriptions and widely adopted applications help your C-level executives understand the progress and flaws of cloud adoption.

DEEP VISIBILITY

Inventories include deep insights of applications, including metadata collected directly from browsers, such as privacy policies, terms and conditions, and social links. HCI provides intelligence, including domain reputation, country of origin, as well as revealing potential phishing or unwanted sites. Scirge also correlates usage trends to discover which services have been popular, trending, or abandoned by your employees, enabling decision-makers to figure out what tools users are missing or favoring for a better digital experience.

ACCOUNT PROTECTION

Employee-created accounts are the Achilles' heel of every organization. Scirge closes the gap between opt-in password managers and opt-in MFA options on third-party sites, and helps to create employee awareness. It is possible to prevent account takeovers, credential misuse, and potential fraud via unveiling what was previously invisible in Shadow IT account usage.



PASSWORD HYGIENE

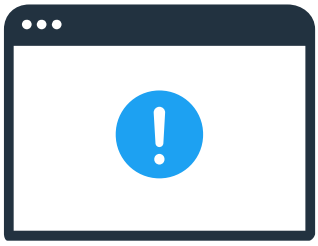
According to NCSC, "Passwords need to be protected within your system, even if the information on the protected system is relatively unimportant." The number one challenge for this is controlling employee-created accounts on third-party websites. This is why each password entered into a browser is rigorously checked for weaknesses by Scirge. Custom complexity rules are available to match regulatory requirements, and the algorithmic password strength is also calculated at the endpoints. Passwords are hashed locally on the endpoint, so their clear form is never sent or stored anywhere else—only industry standard secure hashes are stored at the CMS database, so password reuse, password sharing, or the use of already breached passwords can become visible to your security departments.

AD PASSWORD PROTECTION

In-browser user authentication enables AD/LDAP passwords to go through the same hygiene process, enabling compliance requirements that are often heavier than what AD and other directory services' configurations allow. Identifying AD passwords that are reused in third-party web applications is a red flag indicator of account security, because stolen AD accounts allow seemingly legitimate access to local networks and other integrated cloud services. Protecting your AD accounts should be your top priority, as industry analysts agree that stolen credentials are used in 80% of successful attacks.

EMPLOYEE AWARENESS

Password complexity and privacy regulations are tough to manage without proper education. Employee awareness of phishing sites and risky applications should be improved every day, across all business departments and all levels of access. Scirge provides a one-of-a-kind awareness channel that shows messages at the right place and time.



CUSTOMISED LEARNING

Alerts may be configured to trigger based on policy matches, password strength, complexity violations, or the detection of auto-filled passwords. The combination of awareness messages with policy rules for the appropriate account usage – such as blocking distributed emails or blacklisting VIP email addresses for registrations – allows you to protect high-value assets while constantly reminding users of the expected behavior and corporate policies.

AWARENESS AND EDUCATION

In-browser awareness messages allow for an immediate response when employees are accessing unwanted services, or using blacklisted emails (such as VIP, internal, or distributed email accounts) or weak credentials. You can also set up automated awareness campaigns for specific use-cases via our API integrations, ensuring that your employees are warned and educated on multiple channels, such as email or even SMS. Users learn immediately, gaining knowledge based on their actions, rather than classroom-based formal education covering general policies. Scirge also provides metrics showing overall password hygiene, as well as the exact metrics for measuring the success of these training efforts.

COMPLIANCE AND RISK ASSESSMENT

Shadow IT applications should be embraced, because they serve legitimate and valuable purposes for employees and business departments. Without visibility into these services, however, your organization cannot assess privacy requirements, delegate data ownership, plan business continuity, or conduct business impact analysis.

RISK ASSESSMENT

Scirge detects when the accounts of VIP users, ex-employees, or otherwise important users are being accessed by others, unveiling potential impersonation and insider threats. When multiple employees are using the same credentials, conflicts over the segregation of duties arise in the breach of several regulatory requirements. These shared accounts are highly relevant for internal web applications as well – especially in the financial and HR departments, but also for high-privilege users and IT staff. Users accessing an unusually high number of apps or providing a lower-than-required password strength may also be flagged, either for review of conduct or assignment to further training.

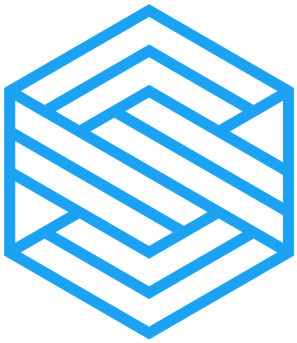
AUTOMATIC TERMS COLLECTION

Scirge collects privacy policies and T&Cs from all applications that employees access which are monitored via policies. By combining usage trends, such as popularity, with geographic data and reputation, compliance departments can identify which services are potentially critical or risky. Terms of these services may then be evaluated and integrated with existing corporate policies, while users may be warned and educated for proper use. Illuminating Shadow IT turns it into a controlled and manageable part of your technological ecosystem, lowering your regulatory exposure.

FEATURE MATRIX

ARCHITECTURE AND INTEGRATIONS	SCIRGE ESSENTIALS	SCIRGE 360
Syslog Integration	Yes	Yes
SMTP Integration	Yes	Yes
AD/LDAP Integration	Yes	Yes
API Integration	Yes	Yes
Role Based Access Control	Yes	Yes
PII Anonymization	Yes	Yes
Customizable Alerting	Yes	Yes
WEB APP INVENTORY AND INTELLIGENCE		
Detect Any Web App	Yes	Yes
Automatic Metadata Collection	Yes	Yes
User-level App & Account Inventory	Yes	Yes
Application Usage Intelligence	Yes	Yes
Web App Reputation & Metadata Enrichment	HCI Add-on	Yes
ACCOUNT PROTECTION AND AWARENESS		
Password Strength & Complexity Checks	Yes	Yes
Password Reuse Detection	Yes	Yes
Breached & Common Password Detection	HCI Add-on	Yes
AD Password Strength & Complexity Checks	ADPP Add-on	Yes
AD Password Reuse Detection	ADPP Add-on	Yes
Breached & Common AD Password Detection	HCI & ADPP Add-on	Yes
Custom Password Blacklist Checks	Yes	Yes
In-browser Real-time Awareness Messages	Yes	Yes
Email & API-based Alerts	Yes	Yes
COMPLIANCE AND RISK ASSESSMENT		
Shared Account Detection	Yes	Yes
Identity Misuse Detection	Yes	Yes
Inactive & Disabled AD Account Reuse Detection	Yes	Yes
Power User Detection	Yes	Yes
Automatic Terms & Privacy Policy Collection	Yes	Yes
Blocking Capability	Yes	Yes
LICENSING		
All Future Features Included*	No	Yes
Subscription & Perpetual Licensing Options	Yes	Yes
ADD-ONS		
Multi-browser Add-on (MBA)	Sold Separately	Included
Horizon Cloud Intelligence (HCI)*	Sold Separately	Included
Active Directory Password Protection (ADPP)	Sold Separately	Included
MAINTENANCE		
Subscription License	Included	Included
Perpetual License	Yearly Maintenance	Yearly Maintenance
PRICING	Ask for a Quote	Ask for a Quote

**Valid maintenance Is required for Perpetual licenses*



SCIRGE

SHEDDING LIGHT ON SHADOW IT