SCIRGE

SHEDDING LIGHT ON SHADOW IT

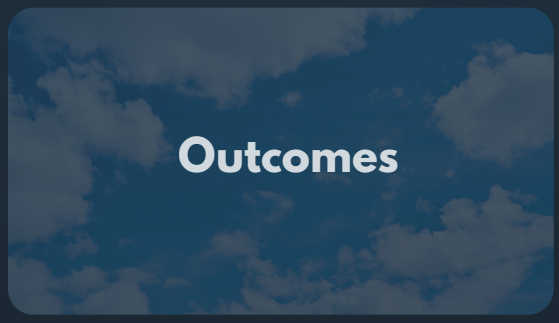
Web applications and accounts that are uncontrolled by IT pose challenges from compliance, password hygiene, data leak, and cost perspective.

Scirge was designed to discover, monitor, analyze, and collect the account information provided by employees on third-party websites and educate them for better security behavior.

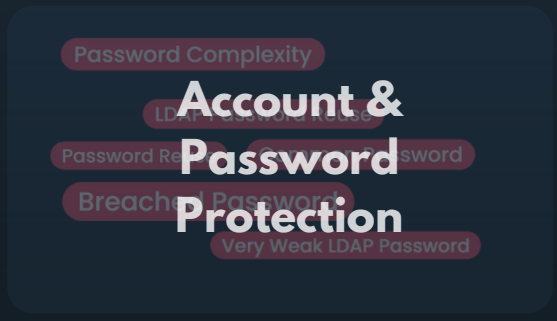
There are approximately 250,000 new domains registered every day. Each of them is a potential Shadow IT application.

Contents

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.



Use Cases



More

What is Your Outcome?

Board

Agile teams and individuals bring about innovation without diligence for security, compliance, or cost-effectiveness. Spear phishing, ransomware attacks, business email compromise, and insider threats are top mentions on all security risk assessments.

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.

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.

Managing third-party identities, and discovering phishing attacks and insecure or breached accounts can provide early warning and prevention for the most frequent and trivial attacks.

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.

Book a Meeting

Shadow IT Discovery & Monitoring

Monitoring

Scirge differentiates websites from SaaS and cloud web applications based on the fact that a user has used a corporate email address or email domain to log in. These URLs are enriched via metadata collected from the browser, as well as dynamic data such as the domain age, blacklist checks, and other domain-related intel. This allows Scirge to build an inventory of all third-party applications without a pre-built database, potentially covering any existing ones. recently created, and even internal web applications.

Deep visibility

Inventories include deep insights into applications, including metadata collected directly from browsers, such as privacy policies, terms and conditions, and social links. Additionally, Horizon Cloud Intelligence provides OSINT-based metadata to pinpoint untrusted, phishing, or otherwise unwanted applications.

Cloud Consumption

Configurable tags with custom thresholds give insight into application usage trends amongst employees. Overlapping subscriptions and widely adopted applications help your C-level executives understand the progress and flaws of cloud adoption.

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 or otherwise at risk, using Horizon Cloud intelligence.

Cloud-security products provide visibility into less than 0,01% of the web.

Start a Trial

Account and Password Protection

Password Hygiene

Employee-created accounts are the Achilles' heel of every organization. Scirge monitors each password entered into a browser to prevent common attack vectors relying on weak credentials, such as account takeovers, phishing, ransomware deployments, and internal fraud. Custom complexity rules are available to match regulatory requirements and industry-standard secure hashing is used to detect password reuse, password sharing, and breached passwords.

Identity Governance

Employee level inventories enable offboarding procedures to extend to third-party accounts, that would otherwise be accessible by ex-employees for an unlimited time, even after departure. Scirge Discovery also allows the detection of browser-saved passwords and accounts that may sync to personal and other unmanaged devices.

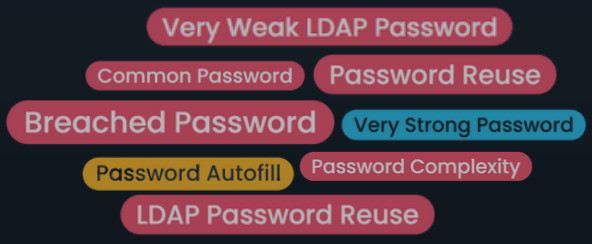
Active Directory Password Protection

Detecting log-ins on Active Directory-connected domains such as Microsoft services or other identity providers is completely transparent for employees. AD/LDAP passwords go through the same process as any other account, enabling complexity checks for compliance and protection. Identifying AD passwords that are reused in third-party web applications is a red flag indicator of account security. Industry analysts agree that stolen credentials are used in 80% of successful attacks, including for ransomware deployments.

Phishing Detection

Account usage, especially LDAP/AD Password reuse on untrusted, or recently registered domains is a strong indicator that employees fell victim to phishing attacks, that were not stopped or discovered by any preventive measures. Scirge has the power to use correlation and intelligence to trigger automated mitigation and education.

"Reuse of passwords means that an attacker can use this information to attempt to access more important accounts, where further damage can be done" -NCSC



Book a Demo

Governance, Risk Management, Compliance

Inventory

Shadow IT applications should be embraced because they serve legitimate and valuable purposes for employees and business departments. Privacy regulations, access, and identity governance, and supplier intelligence coverage are extended to the unmanaged footprint of the organization to decrease your attack surface.

Identity Governance

Visibility into account sharing and usage trends allows the early detection of misconduct or internal fraud. Password hygiene provides peace of mind towards regulation, and decreases the risks of breaches and unsanctioned access via compromised credentials. Offboarding processes are extended to arc over unsanctioned or unmanaged services.

Contextual Visibility

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.

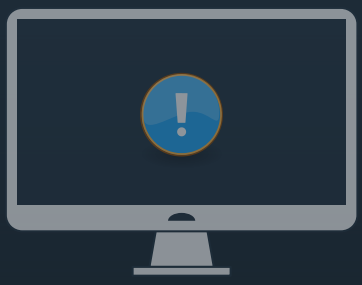
"Migrating to ZTA requires an organization to have detailed knowledge of its assets[...] This includes hardware components [...] and digital artifacts (e.g., user accounts, applications, digital certificates)"
-NIST Zero Trust Guideline

Start a Free Audit

Employee Education and Awareness

Change Behavior

Cyber vigilance starts with great habits and responsible behavior by all departments, regardless of their tech skills. Classroom training for knowledge transfer does not create effective results and is often only a wasteful means for a compliance check. Scirge provides automations that are tailor-made to specific use-cases, and are launched exactly when and to whom it is relevant.



Contextual Learning

According to research, learning is most efficient when the applications or website provides guidance based on the employees' research. Scirge provides in-browser messaging without the need to launch dedicated applications or attend timely sessions.

SMS, Email, and any API-based integration are also at your disposal to create added emphasis and engagement. Templates can include the details of the actions that triggered a notification, so employees know exactly what risks they are involved with, how to properly mitigate them, or where to turn to for additional support and guidance.

Content Based on Needs

Distinct departments, experience, and professional backgrounds require a different approach for education. Scirge allows you to customize your 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.

Measure Success

Password hygiene and other risk factors can be measured and monitored. Employee and group-based progress are tracked to provide feedback about the outcomes of your training program.

"Top sources for seeking information [about security practices] are websites and applications"
-National Cybersecurity Alliance

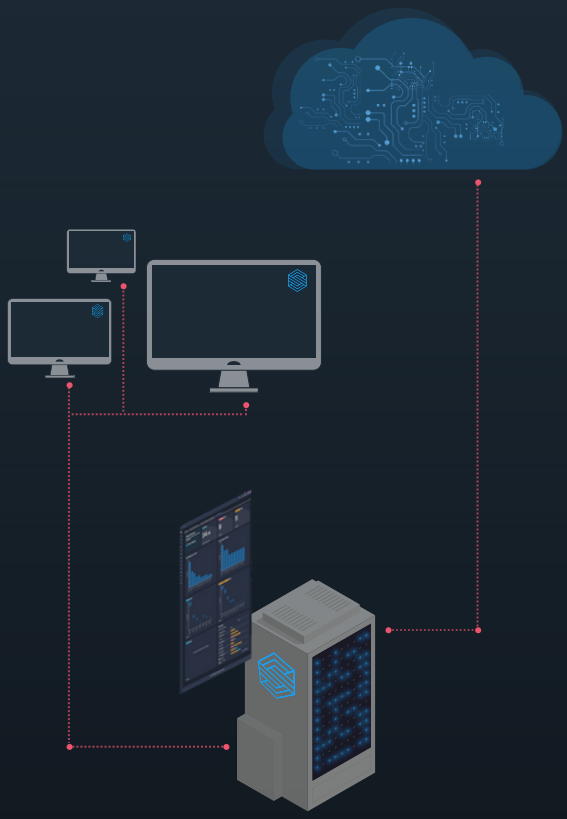
Book a Demo

Architecture and Workflows

Lightweight Implementation

Scirge has a light and unique 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.

Data from the endpoints are collected using secure hashing and encryption at the endpoint, in transit, and at the Central Management Server for maximum privacy. No communication is required by endpoints towards any other cloud or third-party sites.



Contextual and Cloud Intelligence

Data collected on the Central Management Server is enriched by the Horizon Cloud Intelligence feed. Untrusted or risky applications are tagged for compliance and security departments, and usage trends unveil employee requirements for operational and IT decision-makers.

Accounts and password hashes are correlated to discover breached or reused passwords, account sharing, and indicators of potential internal fraud or misconduct, all without ever storing cleartext passwords. Intelligence is provided in the form of easy-to-read tags that can be used for correlation and investigation.

Data Ownership

All data are collected and stored at the Central Management Server, with rigorous configuration for administrator access, encryption, and data retention. Private and business-related usage is differentiated and PII data can be masked to protect employee privacy.

Start a Trial

Features and Licensing

	Scirge Essentials	Scirge 360
SHADOW IT MONITORING		
Web Application Detection	●	●
Usage Trends	●	●
User-level Application & Account Inventories	●	●
Application Risk Intelligence	HCI Add-On	●
SHADOW IT DISCOVERY		
Historic Application Usage Discovery	Discovery Add-on	●
Saved Account Discovery	Discovery Add-on	●
Application Risk Intelligence	Discovery Add-on	●
Zero-Install Discovery	Discovery Add-on	●
ACCOUNT AND PASSWORD PROTECTION		
Password Hygiene for Email-based Accounts		
Password Strength, Complexity, Blacklists Checks	●	●
Password Reuse and Sharing Detection	●	●
Breached & Common Password Detection	HCI Add-On	●
Password Hygiene for Active Directory/LDAP		
Password Strength, Complexity, Blacklists Checks	ADPP Add-On	●
Password Reuse Detection	ADPP Add-On	●
Breached & Common Password Detection	ADPP & HCI Add-On	●
Automation and Workflows		
In-browser Real-time Awareness Notifications	●	●
Email, Syslog, and API-based Workflows and Alerts	●	●
Custom Template based Messages	●	●
COMPLIANCE AND RISK MANAGEMENT		
Internal Threat Detection		
Shared Account Detection	●	●
Identity Misuse Detection	●	●
Private Password Reuse Detection	●	●
Inactive & Disabled AD Account Reuse Detection	●	●
Employee Risk Alerting	●	●
Supply Chain Visibility		
Application Usage Intelligence	●	●
Application Risk Intelligence	HCI Add-On	●
Application Legal Terms Collection	●	●
EMPLOYEE EDUCATION AND AWARENESS		
Multi-channel Messaging	●	●
Employee Profile and Group-based Education	●	●
Automated Reports and Progress Indicators	●	●

Add-ons

Horizon Cloud Intelligence (HCI)
Discovery (DIS)
Active Directory Password Protection (ADPP)

Edpoint Licensese

A single "Scirge Endpoint Browser Extension (EBE) License" includes the right to deploy one agent per each supported browser type, which are running on the same device.

Supported Browsers

Supported OS

Get a Quote