THE CLOUD VISIBILITY GAP

Business requirements change faster than IT organizations are able to adapt. Employee-created processes and services in the cloud undermine visibility, efficiency, and security efforts. Breaking down the web and pinpointing visibility gaps are the first steps to identifying our weaknesses.

Simple Web

With simple websites that have mostly one-way information flow, access is simple and security is not a priority for either providers or users, since no important information is shared or stored in most cases. This is why credential leaks most commonly occur in this category.

- News portals
- Gaming
- Video/media streaming
- Forums
- Personal websites

No visibility, usually no SSO support, mostly personal accounts, credential misuse highly likely.

Cloud Apps

These are services with simple use cases and have a mix of personal and business purposes. Access is easy, with optional MFA or SSO services that may be provided based on user preferences. Services might not be critical from a business perspective. PII and financial data are often collected. Employee-created accounts are also common for productivity purposes.

- Webmail
- Online shopping
- Partner portals
- File sharing
- E-learning
- Booking sites
- Recruitment portals
- Social media

Low-medium visibility, only for SSO-based logins, no API or log available usually.

Enterprise Cloud

Enterprise technologies with highly integrated services and advanced security tools. Access is highly regulated, user roles and authentication methods are controlled via the business organization, and no employee created accounts are possible. MFA and advanced security measures are available.

- CRM/ERP/BI
- Cloud computing
- Cloud virtualization
- Collaboration tools
- Automation
- Industrial services
- Hybrid cloud
- Managed services

High visibility via network, endpoint, API, or identity-based services.

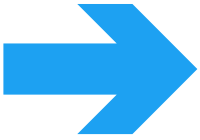
> *CIOs underestimate the number of cloud applications by a factor of 15-22x.*
>
> *—Cisco*

SCIRGE

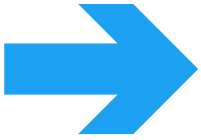
THE ATTACK LIFECYCLE

Credentials are usually not stolen from the multi-billion dollar enterprise cloud providers, but rather from the long tail of the web that has millions of easily accessible services. Employees that utilize these for productivity are creating unmanaged Shadow IT processes and accounts. These invisible credentials contribute to the billions of leaked passwords that can be used in account takeovers, ransomware, and other hacking attacks.

Gain access to personal or business credentials through easy targets.



Reuse credentials for further account takeover, spear phishing, or PII collection.



Reuse accounts, identities, and insights to target high-value assets.

..in terms of how the Ransomware gets on the system... The first vector is through the Use of stolen credentials or Brute force...

—Verizon 2021

ILLUMINATE SHADOW IT

While NGFW/proxy-based solutions can provide almost zero extra protection against Shadow IT, CASB might do a great job protecting the enterprise cloud for certain services. Both approaches, however, lack visibility into and control over Shadow IT across millions of simple websites and cloud apps. These solutions lack account- and person-level inventories and intelligence. Moreover, the absence of proper credential usage monitoring results in blindness towards the reuse of credentials, including high-value AD or LDAP passwords, as well as the use of contextual or breached passwords. This leaves a huge visibility gap that can lead to compliance and management issues, result in additional costs, and make the organizations vulnerable to credential-related threats.

	CASB	NGFW/Proxy	Scirge	Note
App Visibility and Coverage	◗	◔	◕	Scirge provides visibility without databases.
Account Information	◔		●	Scirge provides deep account- and person-level intelligence.
Application Risks	◔	◗	●	Scirge provides risk intel for any third-party web app.
Password Hygiene			●	Scirge provides enterprise-grade password hygiene checks for all accounts
Awareness		◔	●	Scirge provides real-time awareness education based on employee action.
AD Password Protection			●	Scirge provides AD password hygiene checks and reuse monitoring.
Automation and Workflows	◕	◔	●	Scirge provides automation workflows via multiple integrations
Cost of Operation	◗	◗	●	Scirge is lightweight, easy to deploy and operate

ACCESS THE DEMO LAB

GET IN TOUCH

SCIRGE DATASHEET

SCIRGE