STEPS TO CONQUER SHADOW IT

GAIN VISIBILITY

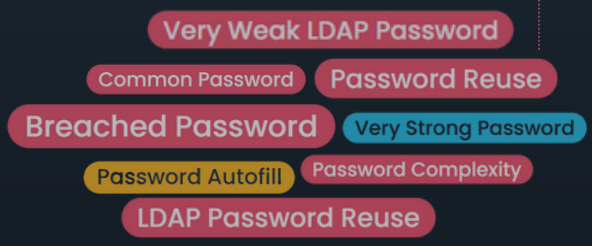
Business requirements change faster than what IT departments can support or adopt. Employee-created processes and services undermine visibility and efficiency.

Illuminate Your Cloud Footprint

- Which applications and suppliers are used by employees without your knowledge?
- What accounts can employees access, even after leaving the company?
- Which applications should be endorsed or blocked by IT departments?

PASSWORD HYGIENE

Unsanctioned, employee-created accounts pose an extreme risk. Account takeovers, ransomware, and hacking attacks all use weak, breached, and insecure credentials.



Each Password Matters

- Is it complex enough?
- Has it been reused multiple times?
- Is it also used for local services?
- Has it been stolen already?

RAISE AWARENESS

Security and compliance start with your employees. Target employees with tailor-made notifications based on their profiles, actions, and skills. This will create lasting change in culture and behavior.

Education Based on Needs

- Are all sites safe to share data through?
- What password complexity is required?
- Should they reuse or share passwords?
- How to identify risky websites and apps?

ENSURE COMPLIANCE

Unknown assets and processes can not be audited for regulatory requirements. Personal, business, and financial data need to stay on your radar. Access rights, roles, and privileges should never stay invisible.

Analyze Your Supply Chain

- Where is your data stored?
- Are accounts being shared?
- What privacy policies and SLAs do your suppliers provide?
- Which users show risky online behavior?

SCIRGE

Get in Touch